Centers for Medicare & Medicaid Services
CMS eXpedited Life Cycle (XLC)

Clinical Lab Fee Schedule (CLFS)

User Manual

Version 5.0

11/23/2021

Document Number: DCCA.FFSDCS.CLFS User Manual.5.0.DRAFT

Contract Number: HHSM-500-2016-00028I

REVISION HISTORY

Version	Date	Point of Contact/Organization	Description of Changes
1.0	09/30/2016	Maureen Campbell/DCCA	Initial Issue
2.0	03/21/2017	Maureen Campbell/DCCA	Updated Introduction content, updated document for CLFS Release 4, added Help Desk, MFA, FAQ, and CLFS Reference Material sections. Made all screenshots 508-compliant. Added Section 7: Reports
3.0	03/30//2017	Maureen Campbell/DCCA	Updated Sections 4 (added sections 4.1 and 4.2), 5 (added 5.2 and 5.2.1 to include Large Volume submissions), 6.1, 7 (added Section 7.1) removed all references to Quick User Guide
4.0	11/15/2019	Maureen Campbell/DCCA	Added Section 5.3 and 5.3.1 to include Very Large Volume submissions.
5.0	10/15/2021	Jennifer Palmer/DCCA	Updated section 4 Laboratory information screenshots to reflect updates to the system. Added figure 4-11. Changed EIDM to IDM throughout document. Other minor copy edits/fact checking

Table of Contents

List of Figures

1. Introduction

1.1 What is the Clinical Laboratory Fee Schedule Data Collection Application?

The Protecting Access to Medicare Act of 2014 (PAMA), required significant changes to how Medicare calculates payment rates for clinical diagnostic laboratory tests (CDLTs) under the Medicare Part B Clinical Laboratory Fee Schedule (CLFS). Beginning January 1, 2018, private payor rates from applicable laboratories became the basis for the revised CLFS.

The CLFS application collects information from applicable laboratories that is used to calculate payment rates for laboratory tests paid on the CLFS. Applicable laboratories, through their reporting entity, must use the CLFS application to submit and certify applicable information, that is, private payor rate data, to the Centers for Medicare & Medicaid Services (CMS).

This document provides guidance that will assist users during the completion of the following processes:

- Register as a CLFS Submitter and CLFS Certifier
- Report Applicable Information
- Certify Reported Applicable Information

1.2 Purpose of the CLFS application

The CLFS application is a component of the Fee-for-Service Data Collection System (FFSDCS).

The CLFS application accepts applicable information from applicable laboratories. The data are validated, stored, and used to calculate payment rates for laboratory tests paid on the CLFS.

The CLFS application supports the following business processes:

- CLFS User Registration
- CLFS Applicable Laboratory Data Reporting
- CLFS Applicable Laboratory Data Certification

The following high-level business requirements for CLFS are implemented:

- Applicable Laboratories through their reporting entity shall report applicable information to CMS
- The CLFS application shall identify consistency errors found in submitted data

1.3 CLFS User Roles

The CLFS application is a role-based application. This means that certain application functions have been linked to specific “user role profiles.” When a new user is given access to the CLFS application, a CLFS role is approved that provides access to the specific functions they need.

- CLFS Submitter: An individual of the Applicable Laboratory who is appointed as data submitter who submits applicable laboratory data through approved file uploads or manual data entry into the CLFS application. The submitter may submit for multiple TINs and will generate a One-Time Password (OTP) for all the TINs to be registered to be shared with the Data Certifier.

This role's objective is for the user to report applicable CDLT and ADLT information to CMS once every 3 years for CDLTs and annually for ADLTs. Below are areas of the CLFS application for which the CLFS Submitter role has access:

  - Applicable Laboratory Registration
    - Requires submission of: Laboratory Name, TIN(s), National Provider Identifier(s) (NPI(s)), and CMS Certification Number (CCN) or Provider Transaction Access Number (PTAN)
    - One Time Password (OTP): User must generate an OTP for all the TINS to be registered, and share this with the CLFS Certifier so that they can successfully complete their registration
  - Data upload
    - CLFS Data Reporting Template: This Comma-Separated Values (.csv) template provides specific data transmission fields for upload into the CLFS application. The .csv file is a pre-defined template (i.e., upload via excel or text file)
    - Upload Data: Best option for laboratories submitting a large amount of data
    - Manual Entry: Best option for laboratories with only a few Healthcare Common Procedure Coding System (HCPCS) codes to submit
  - Status: Status of the applicable information submitted can be found via the "Edit/View Data" page.
  - Validation: Validation is performed for all data submitted. Specific validation rules can be found in Section 5.
  - Corrections (prior to data certification).

- CLFS Certifier: A President or Chief Financial Officer (CFO) of the applicable laboratory, or an individual appointed as data certifier who certifies the accuracy and completeness of applicable information submitted to CMS.
  - Registration: Must receive an OTP from CLFS Submitter to complete registration for all TINs to be registered
  - Certifies data
    - Reviews Data; cannot make edits to data
    - If changes are necessary, CLFS Certifier must inform CLFS Submitter; CLFS Submitter to make any edits
  - Once data are certified, they cannot be viewed or updated by the laboratory

1.4 CLFS Reference Material

The following additional reference materials are utilized to successfully submit and certify applicable data into the CLFS application:

- IDM User Guide
- CLFS Data Reporting Template

Click on IDM Links for any assistance with using the application and to view applicable videos.

2. CLFS Application Access

Users are required to access the CMS Portal at https://portal.cms.gov to begin the registration and role assignment process.

CMS has established the CMS Identity Management (IDM) system to provide our Business Partners with a means to apply for, obtain approval, and receive a single User ID they can use to access one or more CMS applications. The IDM Authentication System prompts the user to create a username and password that conforms to the system’s policies; this user ID and password is not affiliated with the user’s CMS User ID (Enterprise User Administration [EUA]) and password. After the user successfully creates a username and password, the user must create security questions and answers. The user must then re-log in with the new credentials and request the specific FFSDCS CLFS Submitter or CLFS Certifier role as applicable. FFSDCS is a system umbrella that houses various Fee-for-Schedule modules. CLFS is one of the modules under the FFSDCS system.

As part of the role request process the IDM Authentication System begins the Remote Identity Proofing (RIPD) process. RIDP is the process of validating sufficient information about the user (e.g., credit history, personal demographic information, and other indicators) to uniquely identify an individual. After the user’s identity is verified, the CMS Portal pushes the user’s data to CM to review the role request and approve it.

The registration process also involves Multi-Factor Authentication (MFA). This allows the user to authenticate their phone/tablet/PC/laptop, text message Short Message Service (SMS), Interactive Voice Response (IVR), E-mail, and One-Time Security Code.

For additional details on IDM, review the IDM User Guide.

2.1 CLFS Application Access Process

CLFS users with an existing CMS IDM username and password can skip Section 2.1.1 and continue to Section 2.1.2: Requesting CLFS Application Access.

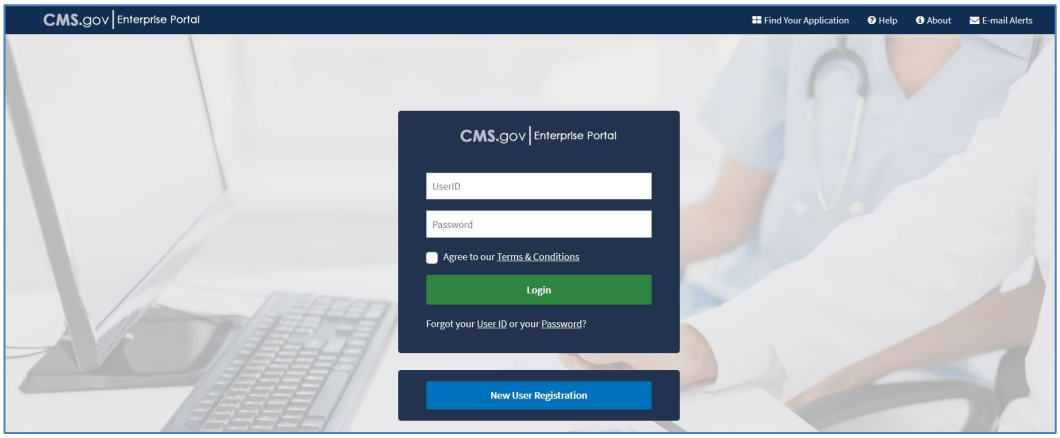
2.1.1 Obtaining a CMS IDM Username and Password

A CMS Portal username and password are required to access the CLFS Application. Perform the following steps to receive the required credentials:

1. Access the CMS Portal: https:\\portal.cms.gov.

   The CMS Portal Home Page is shown in Figure 2-1.

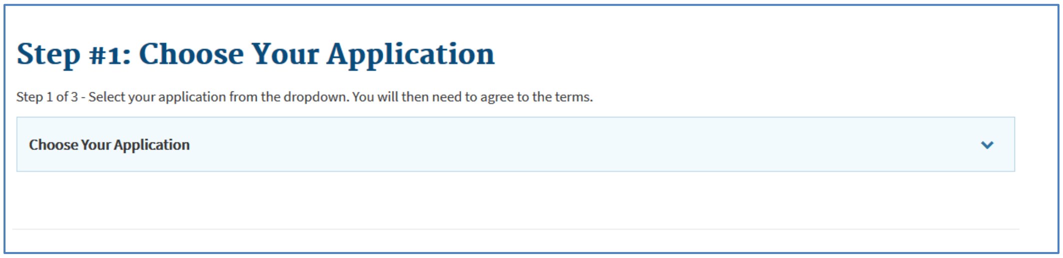
Figure 2-1: CMS Enterprise Portal Home Page


CMS.gov | Enterprise Portal
Find Your Application
Help
About
E-mail Alerts
CMS.gov | Enterprise Portal
UserID
Password
Agree to our Terms & Conditions
Login
Forgot your User ID or your Password?
New User Registration

2. Click on the **New User Registration** button.

   The “Step #1: Choose Your Application” page opens, as shown in Figure 2-2.

Figure 2-2: Step #1: Choose Your Application Page



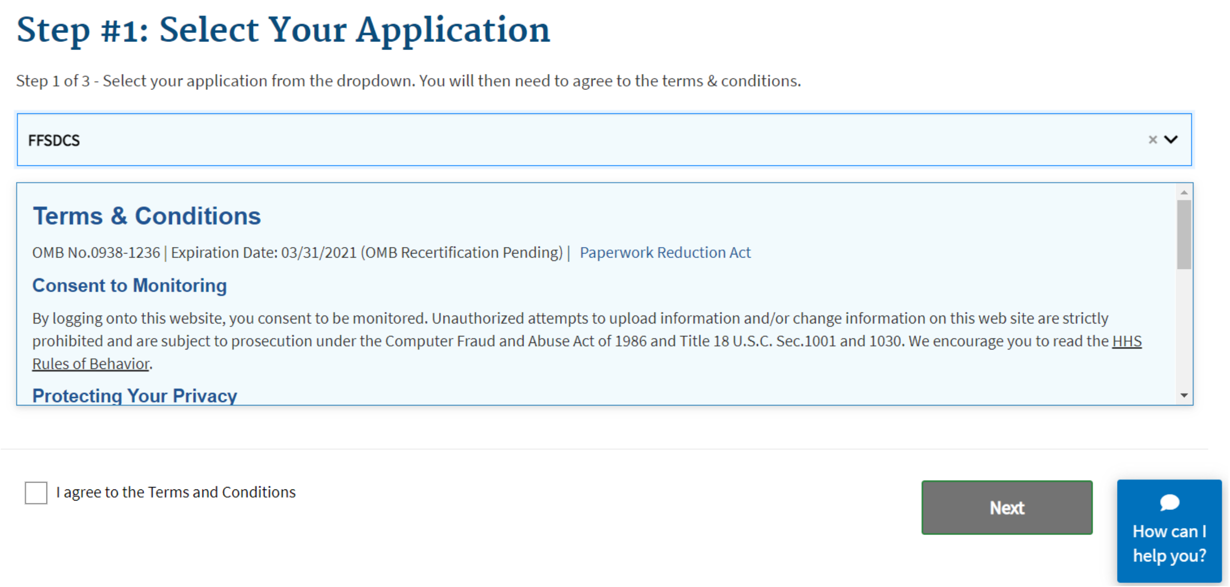
Step #1: Choose Your Application

Step 1 of 3 - Select your application from the dropdown. You will then need to agree to the terms.

3. Select “FFSDCS” from the dropdown list.

   The “Terms and Conditions” page opens, as shown in Figure 2-3.

Figure 2-3: Terms and Conditions Page



Step #1: Select Your Application

Step 1 of 3 - Select your application from the dropdown. You will then need to agree to the terms & conditions.

FFSDCS

Terms & Conditions

OMB No.0938-1236 | Expiration Date: 03/31/2021 (OMB Recertification Pending) | Paperwork Reduction Act

Consent to Monitoring

By logging onto this website, you consent to be monitored. Unauthorized attempts to upload information and/or change information on this web site are strictly prohibited and are subject to prosecution under the Computer Fraud and Abuse Act of 1986 and Title 18 U.S.C. Sec.1001 and 1030. We encourage you to read the HHS Rules of Behavior.

Protecting Your Privacy

□ I agree to the Terms and Conditions

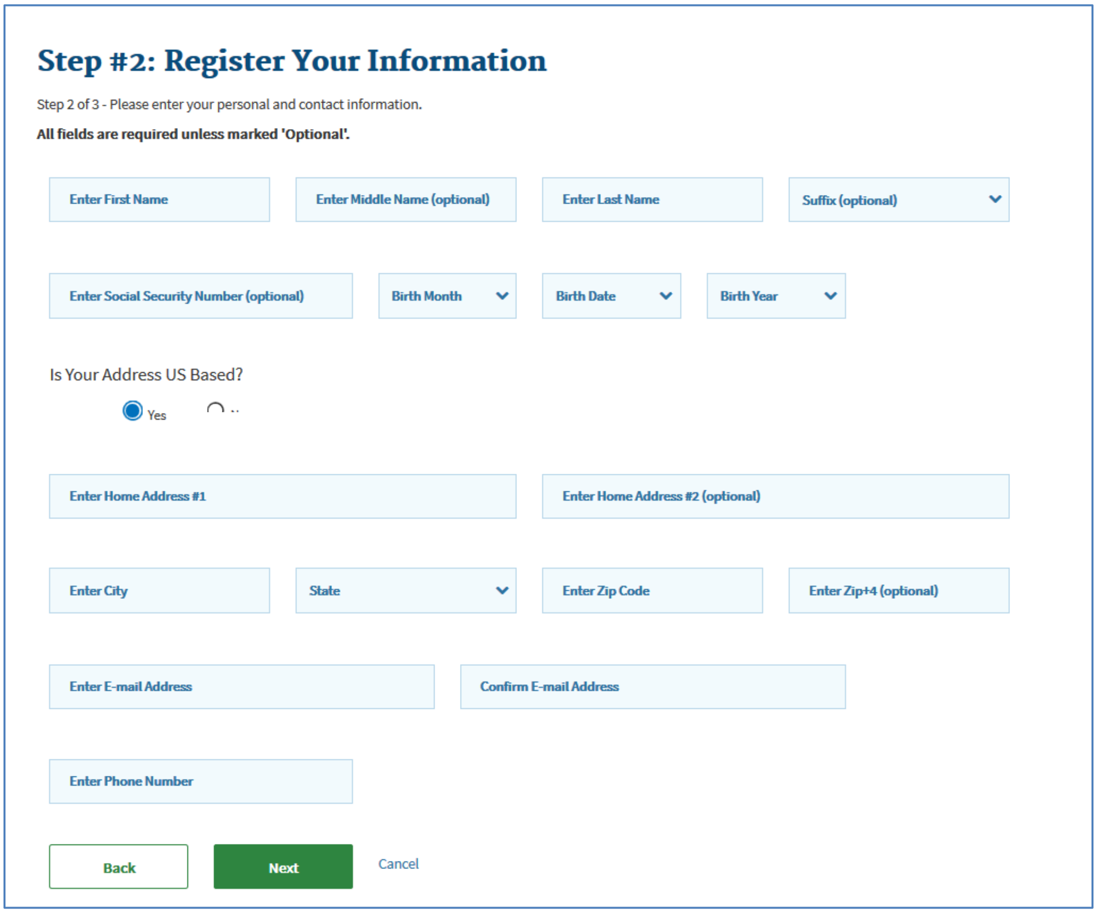
Note: Read through the Terms and Conditions on the page. The page states that you consent to monitoring while accessing and using this website. The page also details the reasons for collecting Personal Identifiable Information (PII); this information is only used to uniquely identify the new user who is registering with the application. The page provides links to the *HHS Rules of Behavior* and the *CMS Privacy Act Statement*.

4. If you agree to the terms and conditions, click the corresponding check box, and click on the **Next** button.

   Note: Users must agree to the terms and conditions to continue the registration process.

   The “Step #2: Register Your Information” page opens, as shown in Figure 2-4.

Figure 2-4: Step #2: Register Your Information Page



Step #2: Register Your Information

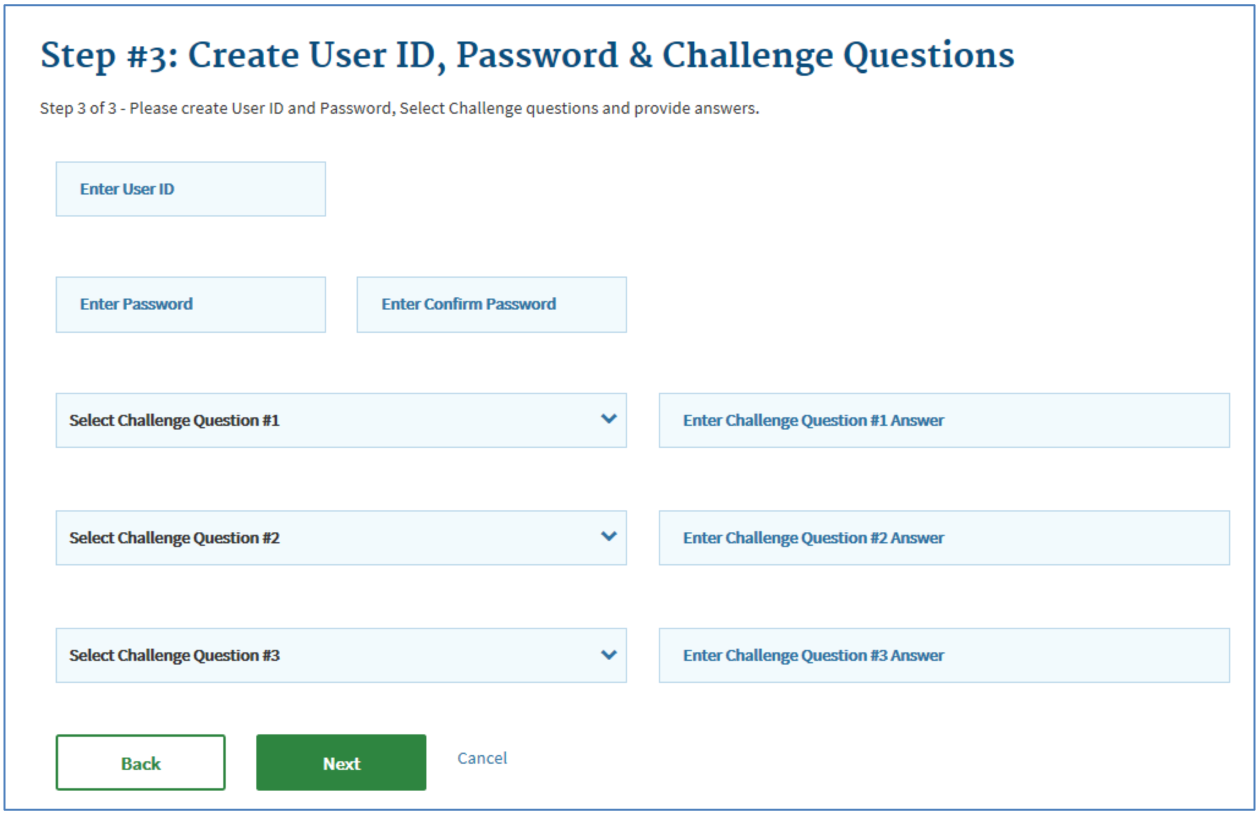
Step 2 of 3 - Please enter your personal and contact information.

All fields are required unless marked 'Optional'.

5. Enter your personal information in the required fields which are indicated by an asterisk (the additional fields are optional but may be required for further identity verification) and click on the **Next** button.

   The “Step 3: Create User ID, Password & Challenge Questions” page display, as shown in Figure 2-5.

Figure 2-5: Step #3: Create User ID, Password & Challenge Questions Page



Step #3: Create User ID, Password & Challenge Questions

Step 3 of 3 - Please create User ID and Password, Select Challenge questions and provide answers.

Enter User ID
Enter Password
Enter Confirm Password
Select Challenge Question #1
Enter Challenge Question #1 Answer
Select Challenge Question #2
Enter Challenge Question #2 Answer
Select Challenge Question #3
Enter Challenge Question #3 Answer
Back
Next
Cancel

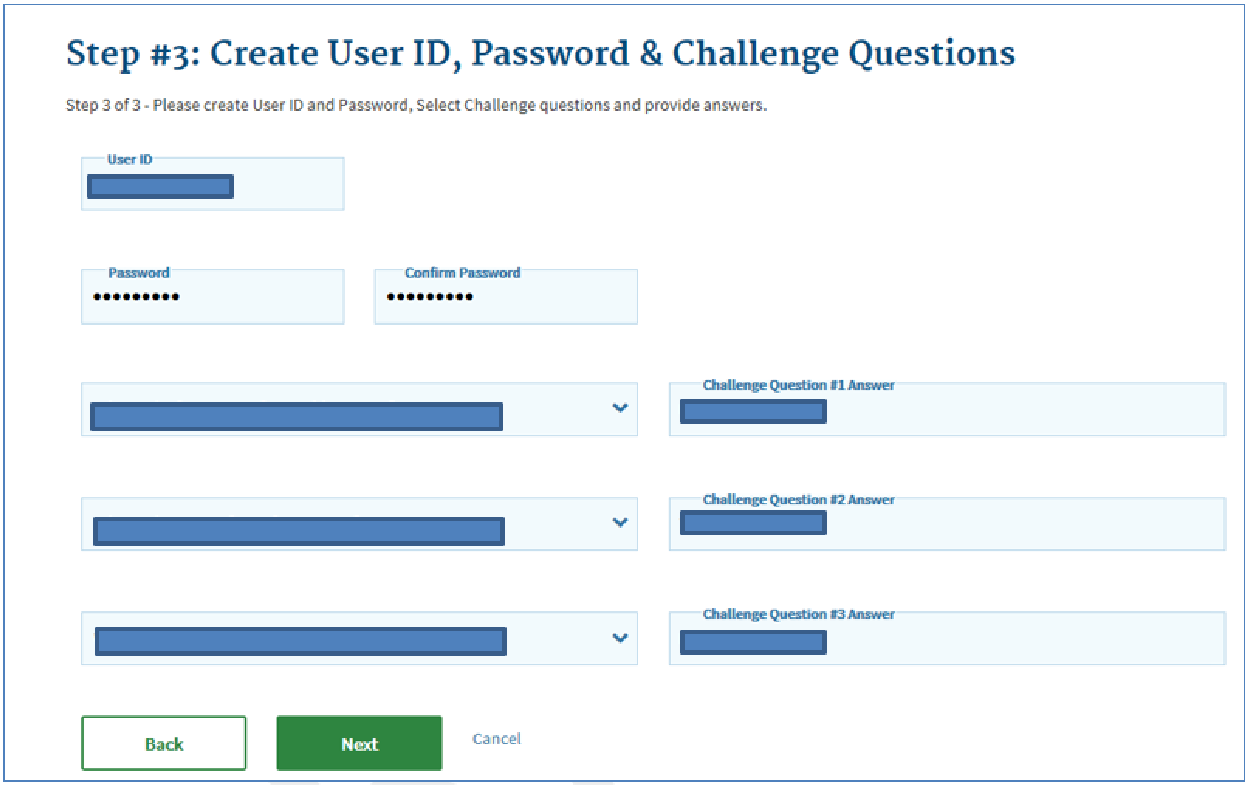
6. Enter your desired User ID in the “User ID” field. The User ID must be a minimum of 6 and a maximum of 74 alphanumeric characters. Allowed special characters are dashes (-), underscores (_), apostrophes (‘), @ and periods (.).
7. Enter your desired password in the “Password” field. The CMS Portal password must conform to the following CMS Acceptable Risk Safeguards (ARS) Password Policy:
   a. Be changed at least every sixty (60) days.
   b. Be a minimum of eight (8) and a maximum of twenty (20) characters.
   c. Be changed only once every 24 hours.
   d. Contain at least one (1) letter, one (1) number, and (1) special character.
   e. Contain at least one (1) uppercase and one (1) lowercase letter.
   f. Not contain your User ID.
   g. Be different from your previous six (6) passwords.
   h. Not contain commonly used words; and
   i. The following special characters may not be used: ? < > ( ) ‘ “ / \ &
8. Re-enter your desired password in the “Confirm Password” field.

   Note: The passwords must match before you can continue.
9. Select a Security Question from each of the three (3) dropdown lists for which the answer is known.

10. Enter the answers to the Security Questions in the corresponding “Answer” fields.

    The fields populate as shown in Figure 2-6.

Figure 2-6: Step #3: Create User ID, Password & Challenge Questions Page Populated



Step #3: Create User ID, Password & Challenge Questions

Step 3 of 3 - Please create User ID and Password, Select Challenge questions and provide answers.

User ID: [redacted]

Password: •••••••••

Confirm Password: •••••••••

[redacted] Challenge Question #1 Answer: [redacted]

[redacted] Challenge Question #2 Answer: [redacted]

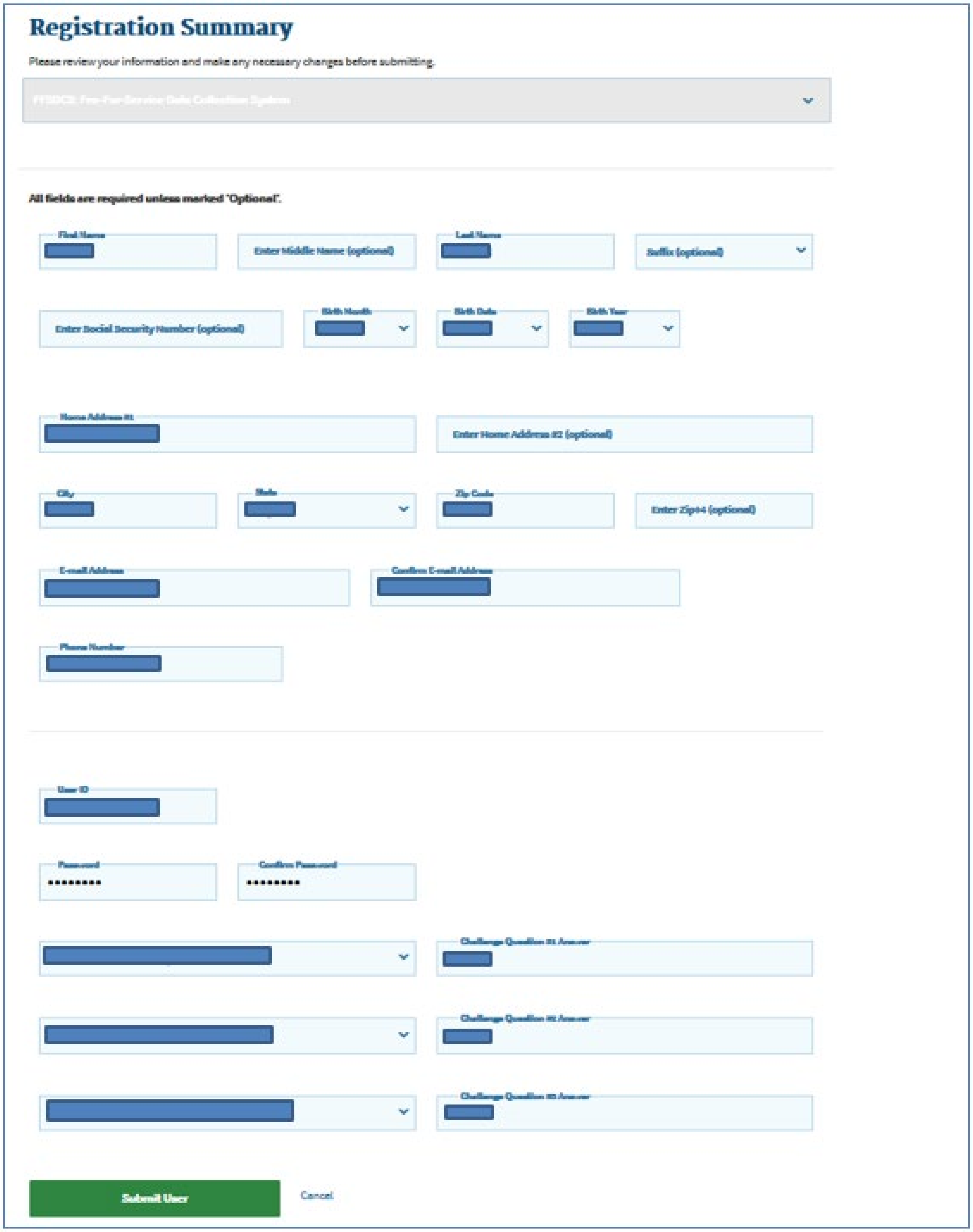
[redacted] Challenge Question #3 Answer: [redacted]

11. Click on the **Next** button to complete the registration process.

    Note: You may click on the **Cancel** button to exit out of the registration process. New information or changes entered will not be saved.

    The “Registration Complete” screen displays as shown in Figure 2-7.

Figure 2-7: Registration Summary Page



Registration Summary

Please review your information and make any necessary changes before submitting.

FFSDCS: Fee-For-Service Data Collection System

All fields are required unless marked 'Optional'.

First Name: [redacted]

Enter Middle Name (optional)

Last Name: [redacted]

Suffix (optional)

Enter Social Security Number (optional)

Birth Month: [redacted]

Birth Date: [redacted]

Birth Year: [redacted]

Home Address #1: [redacted]

Enter Home Address #2 (optional)

City: [redacted]

State: [redacted]

Zip Code: [redacted]

Enter Zip+4 (optional)

E-mail Address: [redacted]

Confirm E-mail Address: [redacted]

Phone Number: [redacted]

User ID: [redacted]

Password: ••••••••

Confirm Password: ••••••••

[redacted]

Challenge Question #1 Answer: [redacted]

[redacted]

Challenge Question #2 Answer: [redacted]

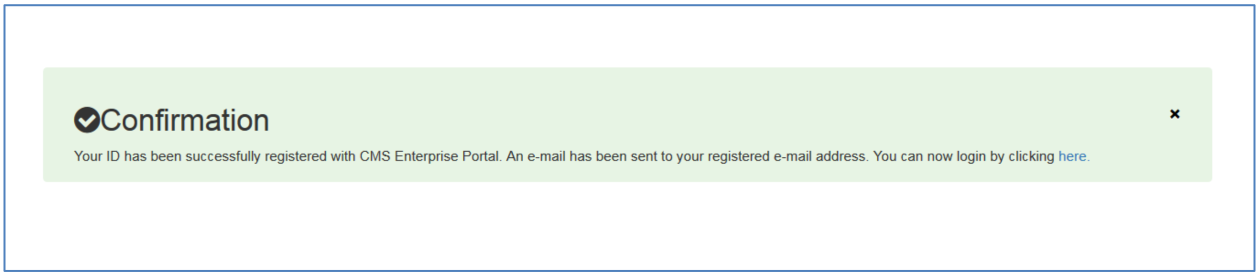
[redacted]

Challenge Question #3 Answer: [redacted]

12. Review, your information, make any necessary changes, and click on the **Submit User** button to complete the registration process.

    A "Confirmation" message displays as shown in Figure 2-8.

Figure 2-8: Confirmation Message



Confirmation

Your ID has been successfully registered with CMS Enterprise Portal. An e-mail has been sent to your registered e-mail address. You can now login by clicking here.

13. Please wait at least 5 minutes before logging on to the CMS Portal with your new IDM user ID and password.

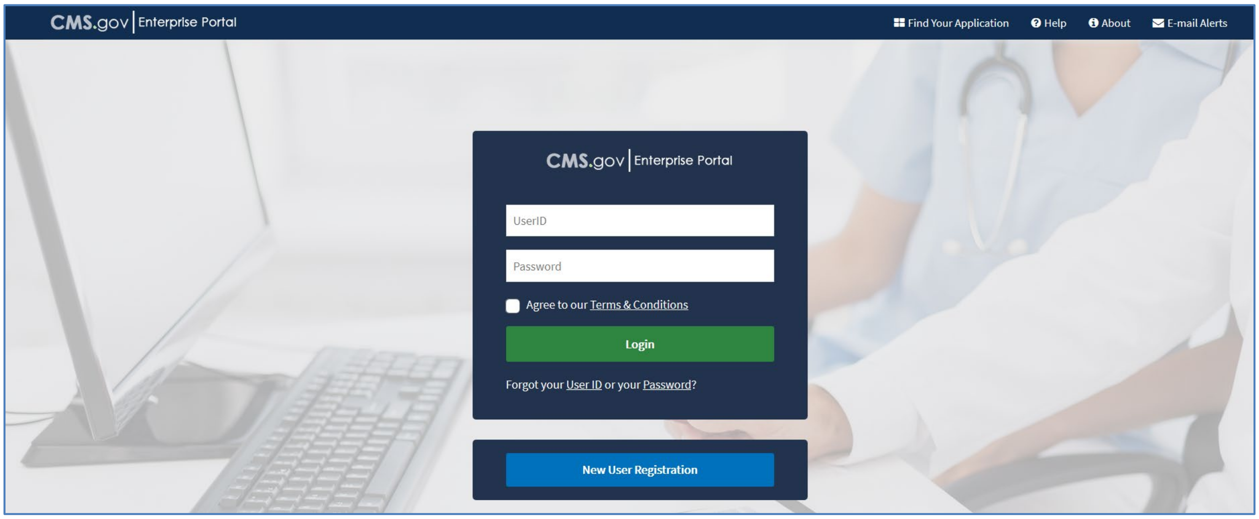
2.1.2 Requesting CLFS Application Access

Perform the following steps to request access to the CLFS application:

1. Enter the address for the CMS portal (https://portal.cms.gov/portal/) into your web browser and click on the **Enter** button.

   The CMS Portal Home Page opens as shown in Figure 2-9.

Figure 2-9: CMS Portal Home Page

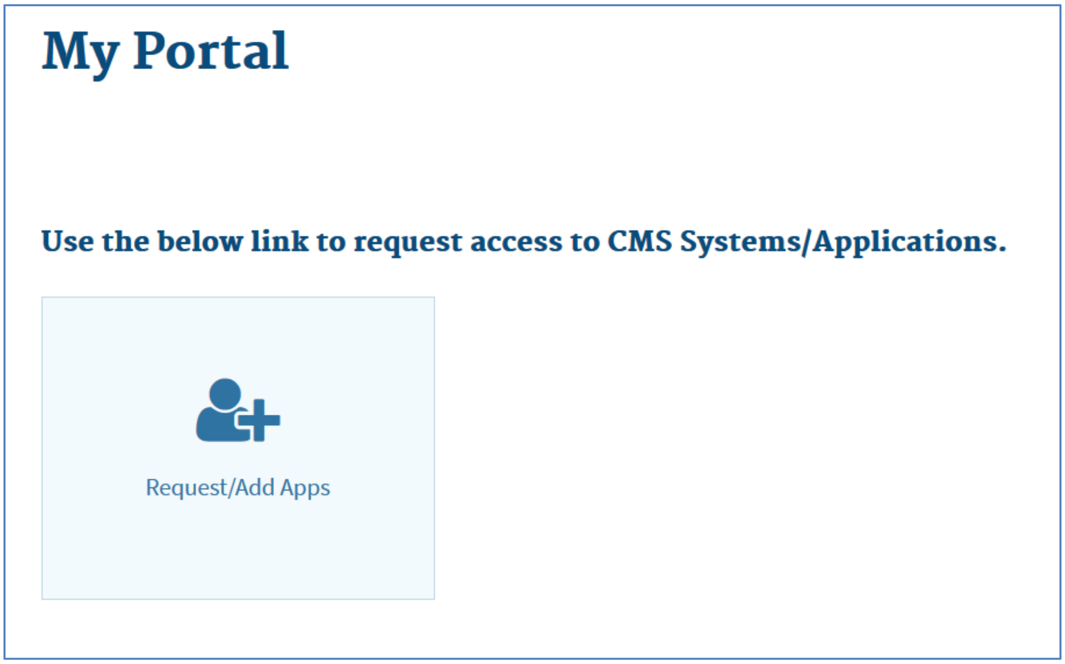


CMS.gov | Enterprise Portal
Find Your Application
Help
About
E-mail Alerts
CMS.gov | Enterprise Portal
UserID
Password
Agree to our Terms & Conditions
Login
Forgot your User ID or your Password?
New User Registration

2. Enter your UserID and Password and click on the **Login** button.

   The “My Portal” page displays, as shown in Figure 2-10.

Figure 2-10: My Portal Page



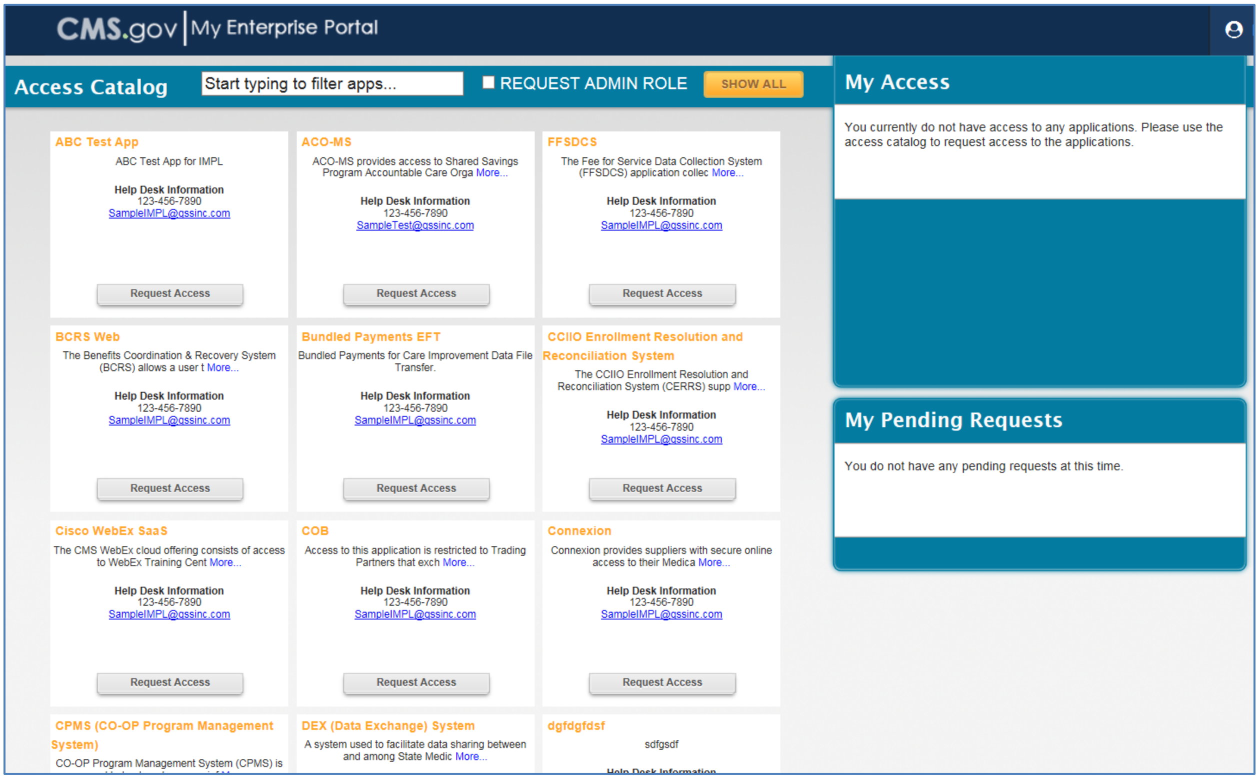
My Portal

Use the below link to request access to CMS Systems/Applications.

3. Click on **Request/Add Apps**.

   The “Access Catalog” page displays, as shown in Figure 2-11.

Figure 2-11: Access Catalog Page



CMS.gov | My Enterprise Portal
Access Catalog
Start typing to filter apps...
□ REQUEST ADMIN ROLE
SHOW ALL

ABC Test App
ABC Test App for IMPL
Help Desk Information
123-456-7890
SampleIMPL@qssinc.com
Request Access

ACO-MS
ACO-MS provides access to Shared Savings Program Accountable Care Orga More...
Help Desk Information
123-456-7890
SampleTest@qssinc.com
Request Access

FFSDCS
The Fee for Service Data Collection System (FFSDCS) application collec More...
Help Desk Information
123-456-7890
SampleIMPL@qssinc.com
Request Access

BCRS Web
The Benefits Coordination & Recovery System (BCRS) allows a user t More...
Help Desk Information
123-456-7890
SampleIMPL@qssinc.com
Request Access

Bundled Payments EFT
Bundled Payments for Care Improvement Data File Transfer.
Help Desk Information
123-456-7890
SampleIMPL@qssinc.com
Request Access

CCIIO Enrollment Resolution and Reconciliation System
The CCIIO Enrollment Resolution and Reconciliation System (CERRS) supp More...
Help Desk Information
123-456-7890
SampleIMPL@qssinc.com
Request Access

Cisco WebEx SaaS
The CMS WebEx cloud offering consists of access to WebEx Training Cent More...
Help Desk Information
123-456-7890
SampleIMPL@qssinc.com
Request Access

COB
Access to this application is restricted to Trading Partners that exch More...
Help Desk Information
123-456-7890
SampleIMPL@qssinc.com
Request Access

Connexion
Connexion provides suppliers with secure online access to their Medica More...
Help Desk Information
123-456-7890
SampleIMPL@qssinc.com
Request Access

CPMS (CO-OP Program Management System)
CO-OP Program Management System (CPMS) is

DEX (Data Exchange) System
A system used to facilitate data sharing between and among State Medic More...

dgfdgfdsf
sdfgsdf
Help Desk Information

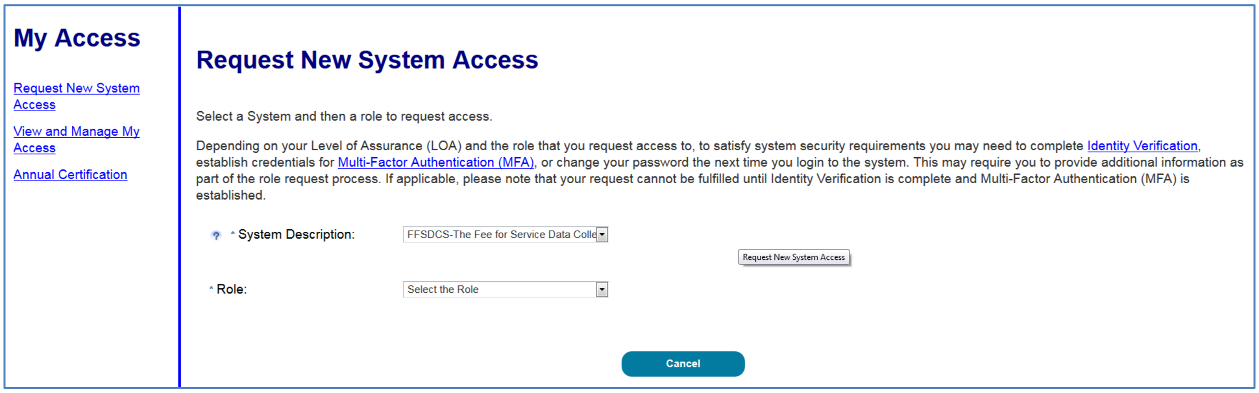
My Access
You currently do not have access to any applications. Please use the access catalog to request access to the applications.

My Pending Requests
You do not have any pending requests at this time.

4. Click on the **Request Access** button in the "FFSDCS" section.

   The "Request New System Access" page displays, as shown in Figure 2-12.

Figure 2-12: CMS Portal Password Page


My Access
Request New System Access
View and Manage My Access
Annual Certification
Request New System Access
Cancel

Request New System Access

Select a System and then a role to request access.

Depending on your Level of Assurance (LOA) and the role that you request access to, to satisfy system security requirements you may need to complete Identity Verification, establish credentials for Multi-Factor Authentication (MFA), or change your password the next time you login to the system. This may require you to provide additional information as part of the role request process. If applicable, please note that your request cannot be fulfilled until Identity Verification is complete and Multi-Factor Authentication (MFA) is established.

* System Description: FFSDCS-The Fee for Service Data Colle

* Role: Select the Role

5. There are two roles that are applicable for CLFS data submission:
   a. CLFS Submitter (who can only submit data)
   b. CLFS Certifier (who can only certify data)

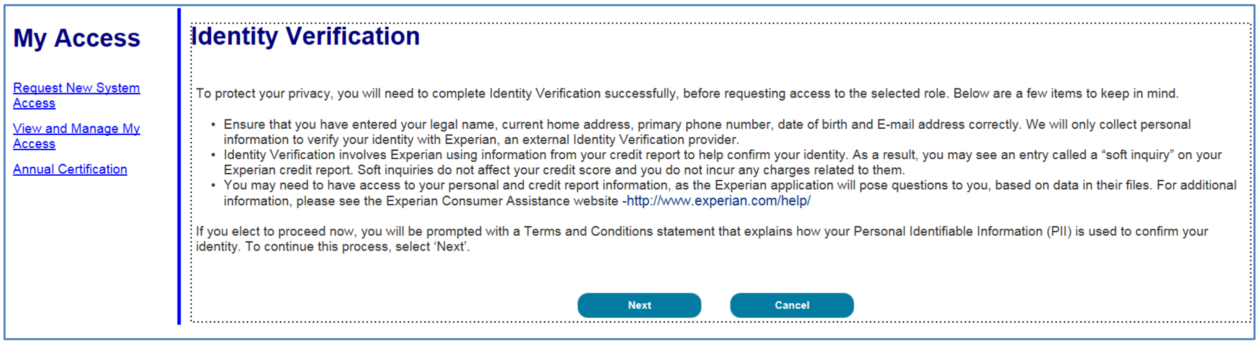
   If your role is only to submit data, and another person will certify, click on the "Role" dropdown list, and select **CLFS Submitter**.

   If your role is to only certify, click on the "Role" dropdown list and select **CLFS Certifier**.

6. If desired, enter any notes to the approver, and click on the **Submit** button

   The "Identify Verification" page displays, as shown in Figure 2-13.

Figure 2-13: CMS Portal Home Page



Identity Verification

To protect your privacy, you will need to complete Identity Verification successfully, before requesting access to the selected role. Below are a few items to keep in mind.

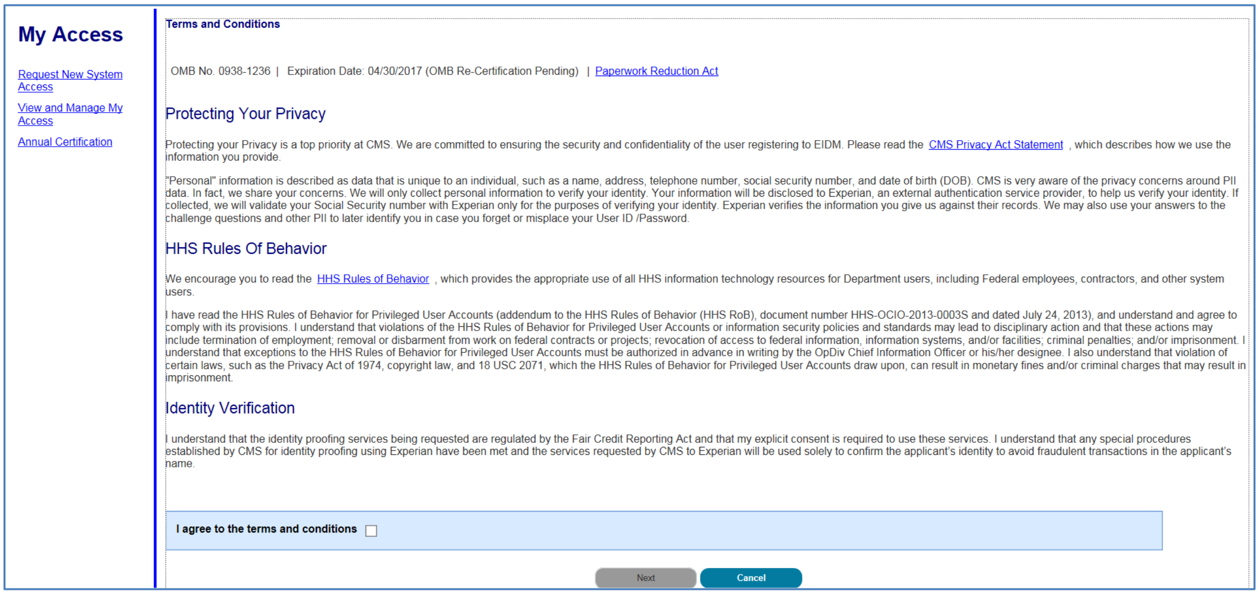
- Ensure that you have entered your legal name, current home address, primary phone number, date of birth and E-mail address correctly. We will only collect personal information to verify your identity with Experian, an external Identity Verification provider.
- Identity Verification involves Experian using information from your credit report to help confirm your identity. As a result, you may see an entry called a "soft inquiry" on your Experian credit report. Soft inquiries do not affect your credit score and you do not incur any charges related to them.
- You may need to have access to your personal and credit report information, as the Experian application will pose questions to you, based on data in their files. For additional information, please see the Experian Consumer Assistance website -http://www.experian.com/help/

If you elect to proceed now, you will be prompted with a Terms and Conditions statement that explains how your Personal Identifiable Information (PII) is used to confirm your identity. To continue this process, select 'Next'.

7. Review the information and click on the **Next** button

   The "Terms and Conditions" page displays, as shown in Figure 2-14.

Figure 2-14: Terms and Conditions Page



Terms and Conditions

OMB No. 0938-1236 | Expiration Date: 04/30/2017 (OMB Re-Certification Pending) | Paperwork Reduction Act

Protecting Your Privacy

Protecting your Privacy is a top priority at CMS. We are committed to ensuring the security and confidentiality of the user registering to EIDM. Please read the CMS Privacy Act Statement , which describes how we use the information you provide.

"Personal" information is described as data that is unique to an individual, such as a name, address, telephone number, social security number, and date of birth (DOB). CMS is very aware of the privacy concerns around PII data. In fact, we share your concerns. We will only collect personal information to verify your identity. Your information will be disclosed to Experian, an external authentication service provider, to help us verify your identity. If collected, we will validate your Social Security number with Experian only for the purposes of verifying your identity. Experian verifies the information you give us against their records. We may also use your answers to the challenge questions and other PII to later identify you in case you forget or misplace your User ID /Password.

HHS Rules Of Behavior

We encourage you to read the HHS Rules of Behavior , which provides the appropriate use of all HHS information technology resources for Department users, including Federal employees, contractors, and other system users.

I have read the HHS Rules of Behavior for Privileged User Accounts (addendum to the HHS Rules of Behavior (HHS RoB), document number HHS-OCIO-2013-0003S and dated July 24, 2013), and understand and agree to comply with its provisions. I understand that violations of the HHS Rules of Behavior for Privileged User Accounts or information security policies and standards may lead to disciplinary action and that these actions may include termination of employment; removal or disbarment from work on federal contracts or projects; revocation of access to federal information, information systems, and/or facilities; criminal penalties; and/or imprisonment. I understand that exceptions to the HHS Rules of Behavior for Privileged User Accounts must be authorized in advance in writing by the OpDiv Chief Information Officer or his/her designee. I also understand that violation of certain laws, such as the Privacy Act of 1974, copyright law, and 18 USC 2071, which the HHS Rules of Behavior for Privileged User Accounts draw upon, can result in monetary fines and/or criminal charges that may result in imprisonment.

Identity Verification

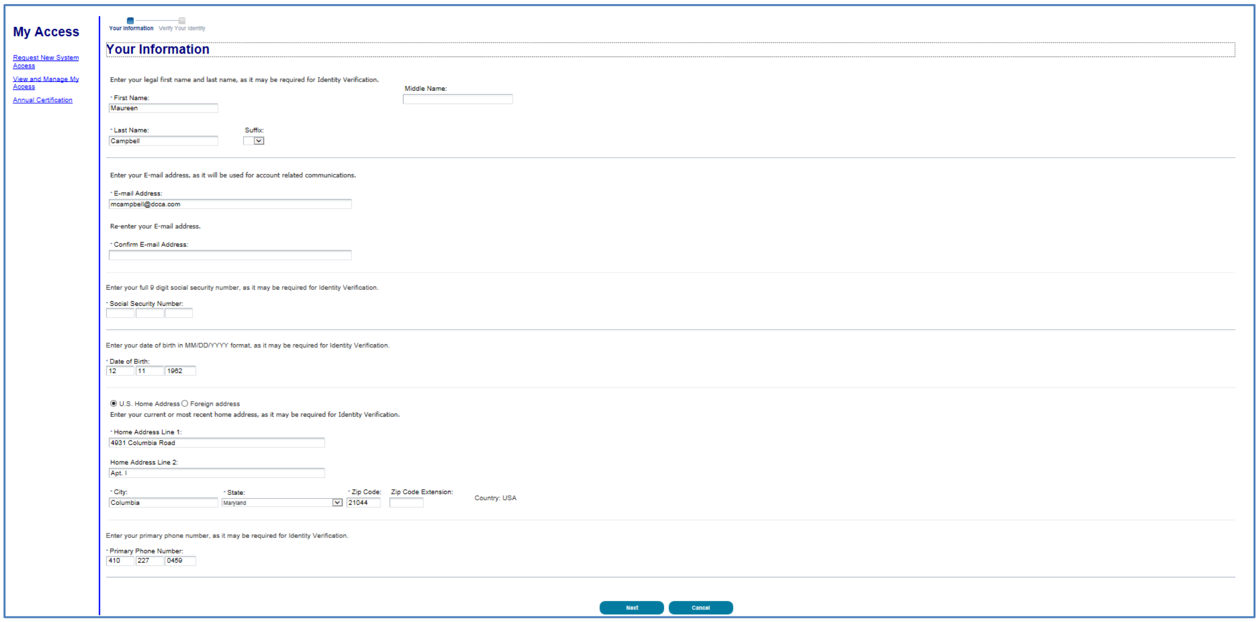
I understand that the identity proofing services being requested are regulated by the Fair Credit Reporting Act and that my explicit consent is required to use these services. I understand that any special procedures established by CMS for identity proofing using Experian have been met and the services requested by CMS to Experian will be used solely to confirm the applicant's identity to avoid fraudulent transactions in the applicant's name.

I agree to the terms and conditions □

8. Review the information, click in the box next to “I agree to the terms and conditions,” and click on the **Next** button.

   The “Your Information” page displays, as shown in Figure 2-15.

Figure 2-15: Your Information Page



Your Information

Enter your legal first name and last name, as it may be required for Identity Verification.

* First Name: Maureen

Middle Name:

* Last Name: Campbell

Suffix:

Enter your E-mail address, as it will be used for account related communications.

* E-mail Address: mcampbell@dcca.com

Re-enter your E-mail address.

* Confirm E-mail Address:

Enter your full 9 digit social security number, as it may be required for Identity Verification.

* Social Security Number:

Enter your date of birth in MM/DD/YYYY format, as it may be required for Identity Verification.

* Date of Birth: 12 11 1962

● U.S. Home Address ○ Foreign address

Enter your current or most recent home address, as it may be required for Identity Verification.

* Home Address Line 1: 4931 Columbia Road

Home Address Line 2: Apt. I

* City: Columbia

* State: Maryland

* Zip Code: 21044

Zip Code Extension:

Country: USA

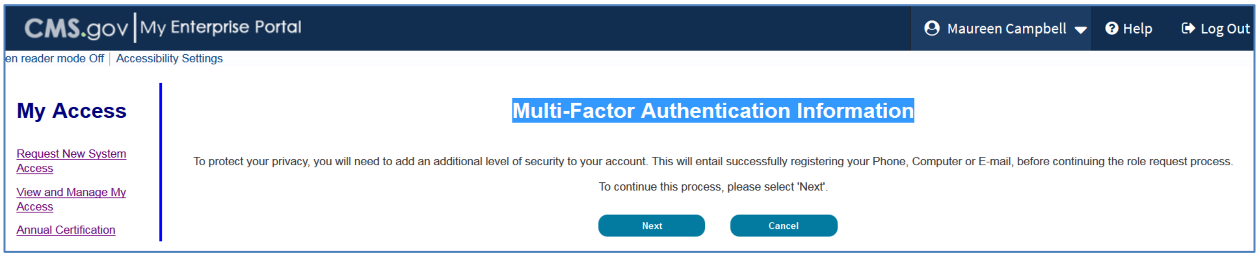
Enter your primary phone number, as it may be required for Identity Verification.

* Primary Phone Number: 410 227 0459

9. Review your information, complete any additional required fields, and click on the **Next** button.

   The “Multi-Factor Authentication Information” page displays, as shown in Figure 2-16.

Figure 2-16: Multi-Factor Authentication Information


CMS.gov | My Enterprise Portal
Maureen Campbell
Help
Log Out
en reader mode Off | Accessibility Settings
My Access
Request New System Access
View and Manage My Access
Annual Certification
Next
Cancel

Multi-Factor Authentication Information

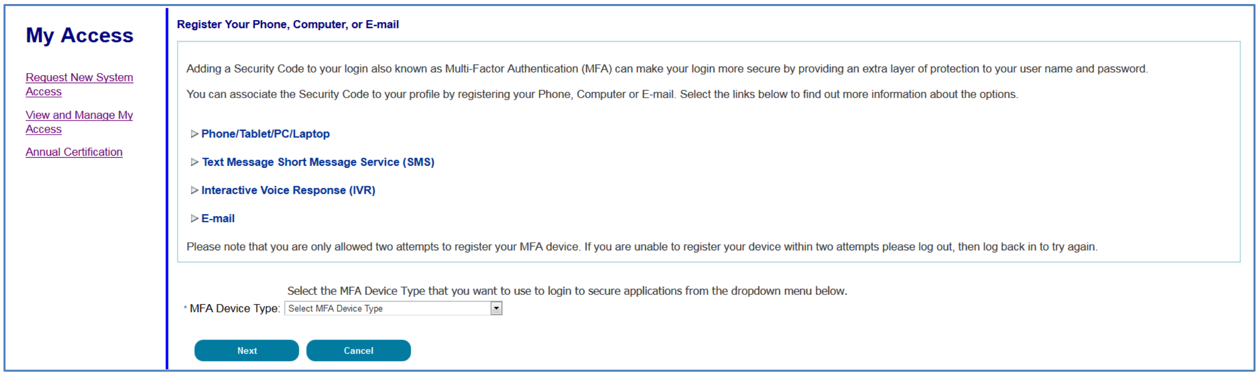
To protect your privacy, you will need to add an additional level of security to your account. This will entail successfully registering your Phone, Computer or E-mail, before continuing the role request process.

To continue this process, please select 'Next'.

10. Click on the **Next** button.

    The “Register Your Phone, Computer, or Email” page displays, as shown in Figure 2-17.

Figure 2-17: Register Your Phone, Computer, or Email Page



Register Your Phone, Computer, or E-mail

Adding a Security Code to your login also known as Multi-Factor Authentication (MFA) can make your login more secure by providing an extra layer of protection to your user name and password.

You can associate the Security Code to your profile by registering your Phone, Computer or E-mail. Select the links below to find out more information about the options.

▷ Phone/Tablet/PC/Laptop

▷ Text Message Short Message Service (SMS)

▷ Interactive Voice Response (IVR)

▷ E-mail

Please note that you are only allowed two attempts to register your MFA device. If you are unable to register your device within two attempts please log out, then log back in to try again.

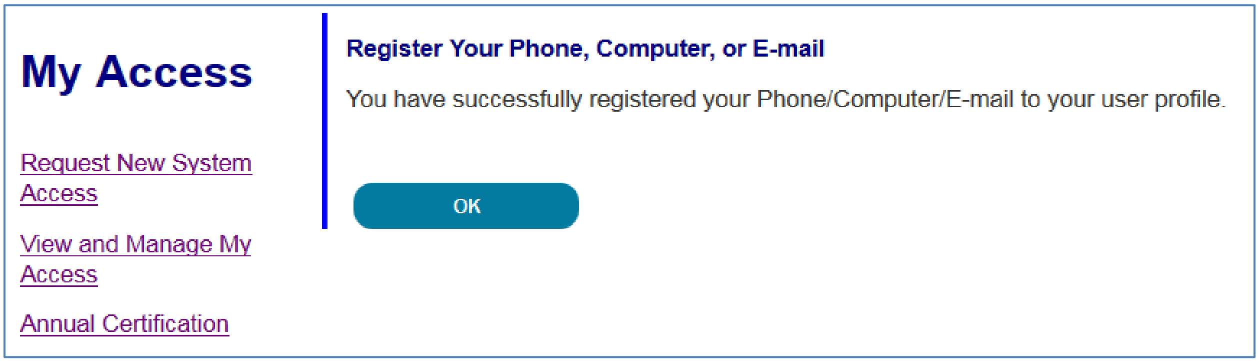
Select the MFA Device Type that you want to use to login to secure applications from the dropdown menu below.

* MFA Device Type: Select MFA Device Type

11. Select a device from the “MFA Device Type” dropdown list, enter any required information requested for the selected device, and click on the **Next** button.

    A message displays that your device has been registered successfully displays, as shown in Figure 2-18.

Figure 2-18: Successful MFA Registration Message



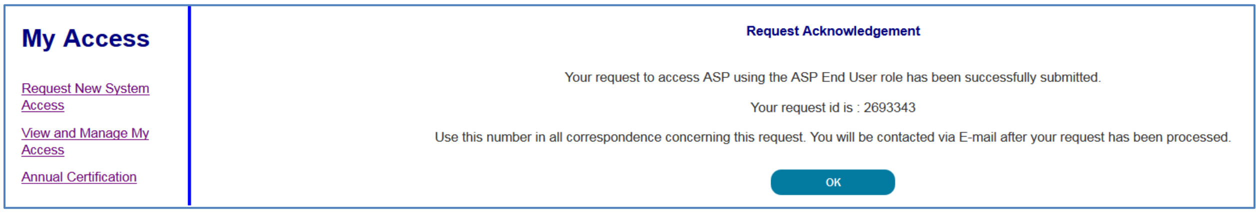
Register Your Phone, Computer, or E-mail

You have successfully registered your Phone/Computer/E-mail to your user profile.

12. Click on the **OK** button.

    A “Request Acknowledgement” screen displays, as shown in Figure 2-19.

Figure 2-19: Request Acknowledgement Page



Request Acknowledgement

Your request to access ASP using the ASP End User role has been successfully submitted.

Your request id is : 2693343

Use this number in all correspondence concerning this request. You will be contacted via E-mail after your request has been processed.

13. Click on the **OK** button.

Note: After role submission, please wait up to 72 hours to receive an e-mail notification.

2.2 Points of Contact

2.2.1 FFSDCS (CLFS) Application Helpdesk

- Email: CLFSHelpDesk@dcca.com
- Phone: 844-876-0765

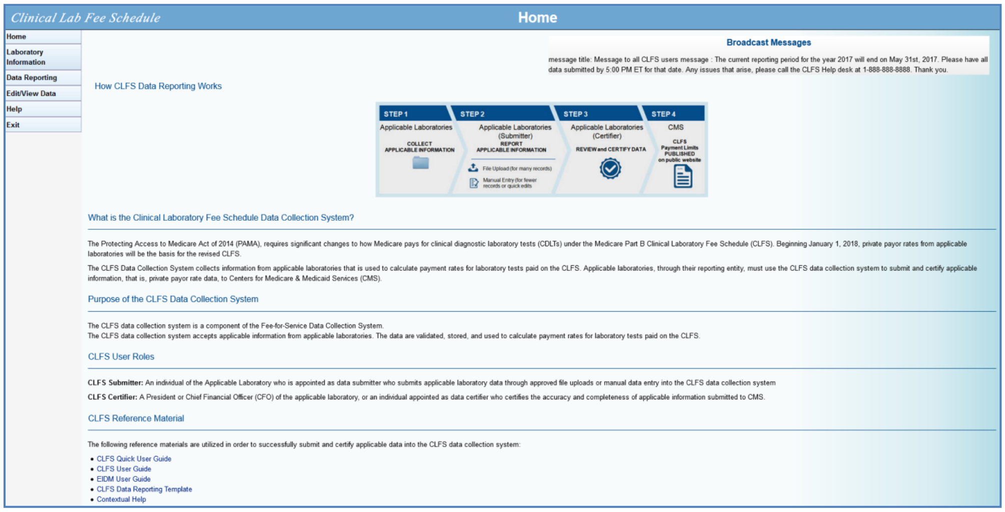
3. CLFS Application Home Page

The CLFS application is comprised of numerous pages and pop-up windows to allow applicable laboratories to report and certify applicable information. The fields displayed on each page differ based on the type of user logged in and the privileges assigned to the user role for the logged in user. The user can enter data into the fields in the CLFS application unless the field is displayed with a gray background.

If the user is new to the application, the user will be placed immediately into the Laboratory Information page to register his or her laboratory information with the CLFS application. If the user has already registered, the user will be placed directly onto Data Collection page (for a CLFS Submitter role) or Certification page (for a CLFS Certifier role).

The CLFS application Home Page displays content based on user role and the privileges assigned to the user role. The CLFS application Home Page Welcome Screen is shown in Figure 3-1 for CLFS Submitters, and Figure 3-2 CLFS Certifiers.

Figure 3-1: CLFS Application Home Page - CLFS Submitter


Clinical Lab Fee Schedule
Home
Home
Laboratory Information
Data Reporting
Edit/View Data
Help
Exit
STEP 1
Applicable Laboratories
COLLECT APPLICABLE INFORMATION
STEP 2
Applicable Laboratories (Submitter)
REPORT APPLICABLE INFORMATION
File Upload (for many records)
Manual Entry (for fewer records or quick edits
STEP 3
Applicable Laboratories (Certifier)
REVIEW and CERTIFY DATA
STEP 4
CMS
CLFS Payment Limits PUBLISHED on public website

Broadcast Messages

message title: Message to all CLFS users message : The current reporting period for the year 2017 will end on May 31st, 2017. Please have all data submitted by 5:00 PM ET for that date. Any issues that arise, please call the CLFS Help desk at 1-888-888-8888. Thank you.

How CLFS Data Reporting Works

What is the Clinical Laboratory Fee Schedule Data Collection System?

The Protecting Access to Medicare Act of 2014 (PAMA), requires significant changes to how Medicare pays for clinical diagnostic laboratory tests (CDLTs) under the Medicare Part B Clinical Laboratory Fee Schedule (CLFS). Beginning January 1, 2018, private payor rates from applicable laboratories will be the basis for the revised CLFS.

The CLFS Data Collection System collects information from applicable laboratories that is used to calculate payment rates for laboratory tests paid on the CLFS. Applicable laboratories, through their reporting entity, must use the CLFS data collection system to submit and certify applicable information, that is, private payor rate data, to Centers for Medicare & Medicaid Services (CMS).

Purpose of the CLFS Data Collection System

The CLFS data collection system is a component of the Fee-for-Service Data Collection System.
The CLFS data collection system accepts applicable information from applicable laboratories. The data are validated, stored, and used to calculate payment rates for laboratory tests paid on the CLFS.

CLFS User Roles

CLFS Submitter: An individual of the Applicable Laboratory who is appointed as data submitter who submits applicable laboratory data through approved file uploads or manual data entry into the CLFS data collection system

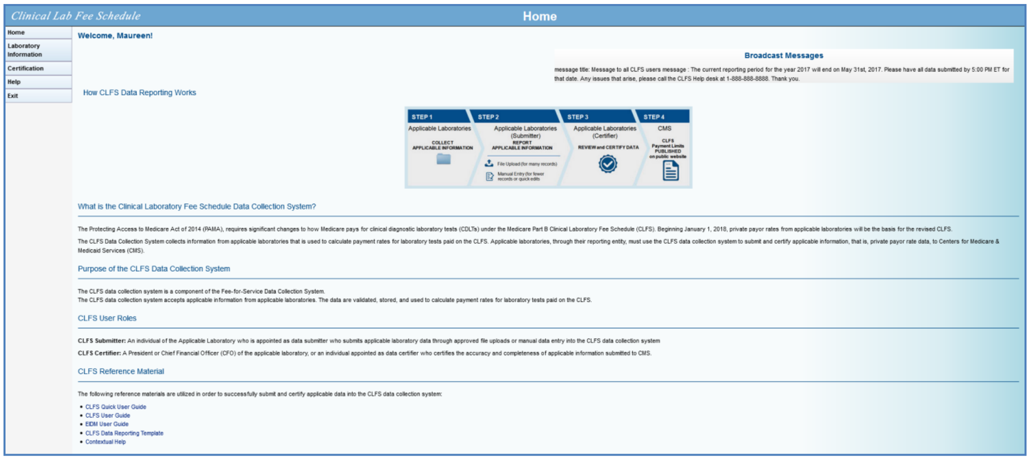
CLFS Certifier: A President or Chief Financial Officer (CFO) of the applicable laboratory, or an individual appointed as data certifier who certifies the accuracy and completeness of applicable information submitted to CMS.

CLFS Reference Material

The following reference materials are utilized in order to successfully submit and certify applicable data into the CLFS data collection system:

- CLFS Quick User Guide
- CLFS User Guide
- EIDM User Guide
- CLFS Data Reporting Template
- Contextual Help

Figure 3-2: CLFS Application Home Page - CLFS Certifier


Clinical Lab Fee Schedule
Home
Home
Laboratory Information
Certification
Help
Exit
STEP 1
Applicable Laboratories
COLLECT APPLICABLE INFORMATION
STEP 2
Applicable Laboratories (Submitter)
REPORT APPLICABLE INFORMATION
File Upload (for many records)
Manual Entry (for fewer records or quick edits
STEP 3
Applicable Laboratories (Certifier)
REVIEW and CERTIFY DATA
STEP 4
CMS
CLFS Payment Limits PUBLISHED on public website

Welcome, Maureen!

Broadcast Messages

message title: Message to all CLFS users message : The current reporting period for the year 2017 will end on May 31st, 2017. Please have all data submitted by 5:00 PM ET for that date. Any issues that arise, please call the CLFS Help desk at 1-888-888-8888. Thank you.

How CLFS Data Reporting Works

What is the Clinical Laboratory Fee Schedule Data Collection System?

The Protecting Access to Medicare Act of 2014 (PAMA), requires significant changes to how Medicare pays for clinical diagnostic laboratory tests (CDLTs) under the Medicare Part B Clinical Laboratory Fee Schedule (CLFS). Beginning January 1, 2018, private payor rates from applicable laboratories will be the basis for the revised CLFS.

The CLFS Data Collection System collects information from applicable laboratories that is used to calculate payment rates for laboratory tests paid on the CLFS. Applicable laboratories, through their reporting entity, must use the CLFS data collection system to submit and certify applicable information, that is, private payor rate data, to Centers for Medicare & Medicaid Services (CMS).

Purpose of the CLFS Data Collection System

The CLFS data collection system is a component of the Fee-for-Service Data Collection System.
The CLFS data collection system accepts applicable information from applicable laboratories. The data are validated, stored, and used to calculate payment rates for laboratory tests paid on the CLFS.

CLFS User Roles

CLFS Submitter: An individual of the Applicable Laboratory who is appointed as data submitter who submits applicable laboratory data through approved file uploads or manual data entry into the CLFS data collection system

CLFS Certifier: A President or Chief Financial Officer (CFO) of the applicable laboratory, or an individual appointed as data certifier who certifies the accuracy and completeness of applicable information submitted to CMS.

CLFS Reference Material

The following reference materials are utilized in order to successfully submit and certify applicable data into the CLFS data collection system:

- CLFS Quick User Guide
- CLFS User Guide
- EIDM User Guide
- CLFS Data Reporting Template
- Contextual Help

4. Laboratory Information

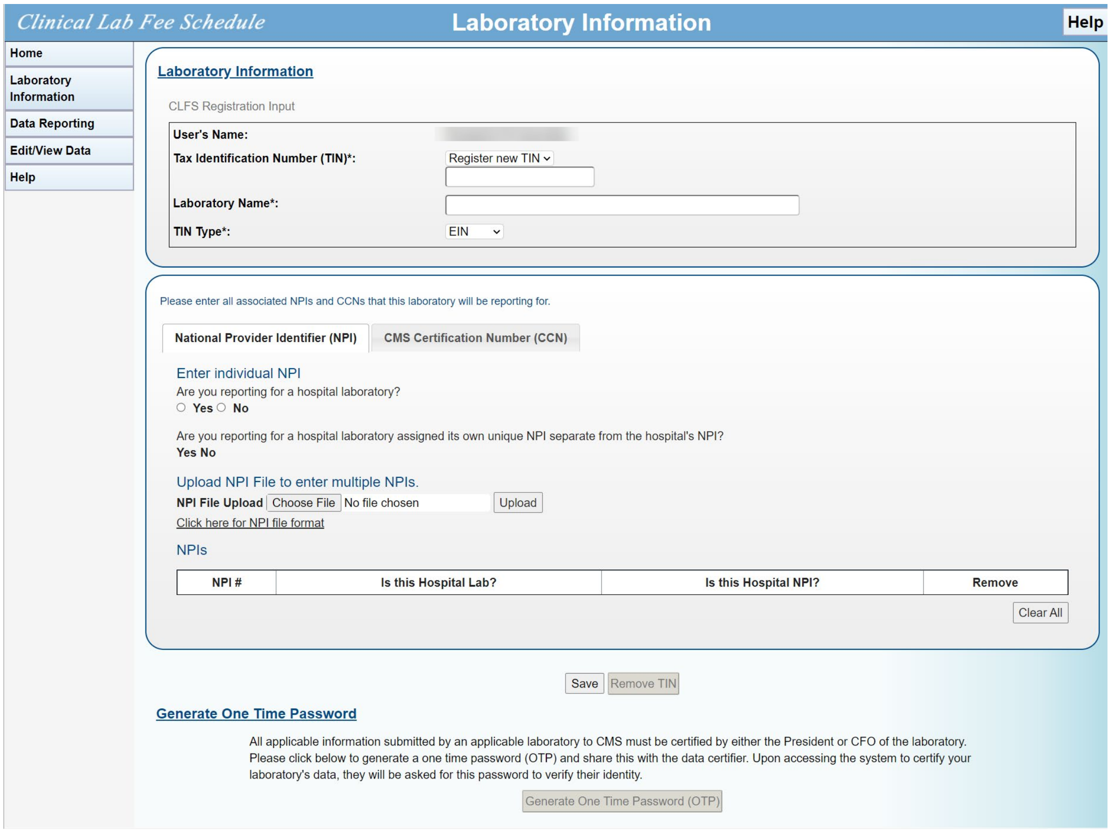
4.1 Add Laboratory Information

The following steps are to be used to enter data into the CLFS application as a CLFS Submitter:

1. Log in to CLFS as CLFS Submitter to open the “Laboratory Information” page.

   The “Laboratory Information” page displays as shown in Figure 4-1.

Figure 4-1: Laboratory Information Page



Clinical Lab Fee Schedule — Laboratory Information — Help

Home
Laboratory Information
Data Reporting
Edit/View Data
Help

Laboratory Information

CLFS Registration Input

User's Name:	[redacted]
Tax Identification Number (TIN)*:	Register new TIN
Laboratory Name*:	
TIN Type*:	EIN

Please enter all associated NPIs and CCNs that this laboratory will be reporting for.

National Provider Identifier (NPI) | CMS Certification Number (CCN)

Enter individual NPI

Are you reporting for a hospital laboratory?

○ Yes ○ No

Are you reporting for a hospital laboratory assigned its own unique NPI separate from the hospital's NPI?

Yes No

Upload NPI File to enter multiple NPIs.

NPI File Upload Choose File No file chosen Upload

Click here for NPI file format

NPIs

NPI #	Is this Hospital Lab?	Is this Hospital NPI?	Remove

Clear All

Save Remove TIN

Generate One Time Password

All applicable information submitted by an applicable laboratory to CMS must be certified by either the President or CFO of the laboratory. Please click below to generate a one time password (OTP) and share this with the data certifier. Upon accessing the system to certify your laboratory's data, they will be asked for this password to verify their identity.

Generate One Time Password (OTP)

2. Enter the following:
   - TIN (use the same TIN entered when completing IDM registration. There are instructions in step 4 for registering multiple TINs.)
   - Laboratory Name
     - One CLFS Submitter and One CLFS Certifier per TIN is allowed
     - A Submitter may be registered for multiple TINs
   - TIN type (either Employer Identification Number [EIN] or Other).
   - NPI – Answer the question ‘Are you reporting for a hospital laboratory?‘ (Yes or No), if Yes, another question will follow ‘Are you reporting for a hospital laboratory assigned its own unique NPI separate from the hospital's NPI?’ (Yes or No). You then can add NPI’s one at a time and click on the **add** button. If you

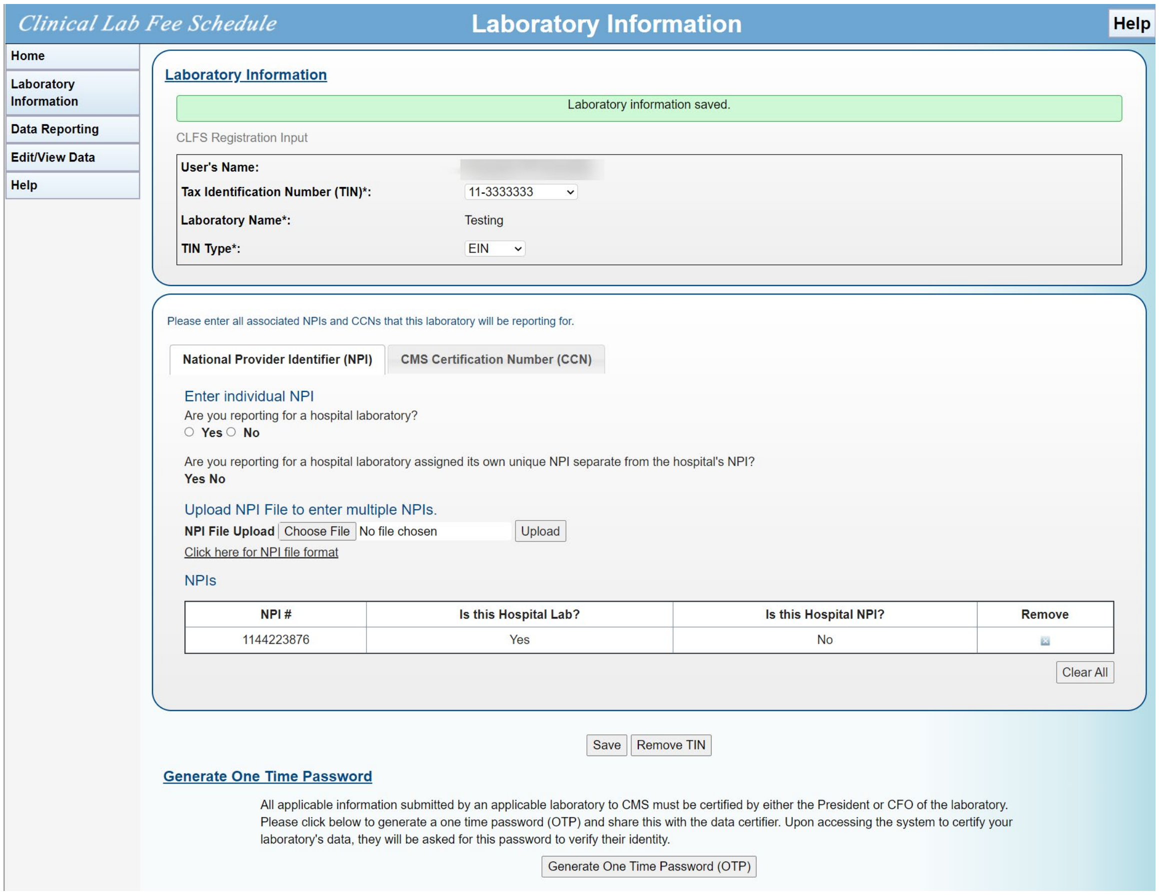
have many NPI's, you can upload a file with them while answering the two questions. You would click on the 'Click here for NPI file format' for the file template, save the file and select the file to upload and click on the **Upload** button

- CCN, add CCN one at a time, select type of CCN (CCN, PTAN or Other) from drop-down list, and click on the **add** button. If you have many CCN's, you can upload a file with them while entering the CCN type. You would click on the 'Click here for CCN file format' for the file template, save the file and select the file to upload and click on the **Upload** button)

3. Click on the **Save** button.

   A message appears stating that the laboratory information has been saved successfully, as shown in Figure 4-2.

Figure 4-2: Laboratory Information – Laboratory Information Saved Page



Laboratory Information

Laboratory information saved.

CLFS Registration Input

User's Name:	[redacted]
Tax Identification Number (TIN)*:	11-3333333
Laboratory Name*:	Testing
TIN Type*:	EIN

Please enter all associated NPIs and CCNs that this laboratory will be reporting for.

National Provider Identifier (NPI) | CMS Certification Number (CCN)

Enter individual NPI

Are you reporting for a hospital laboratory?
○ **Yes** ○ **No**

Are you reporting for a hospital laboratory assigned its own unique NPI separate from the hospital's NPI?
Yes No

Upload NPI File to enter multiple NPIs.

NPI File Upload Choose File No file chosen Upload

Click here for NPI file format

NPIs

NPI #	Is this Hospital Lab?	Is this Hospital NPI?	Remove
1144223876	Yes	No	

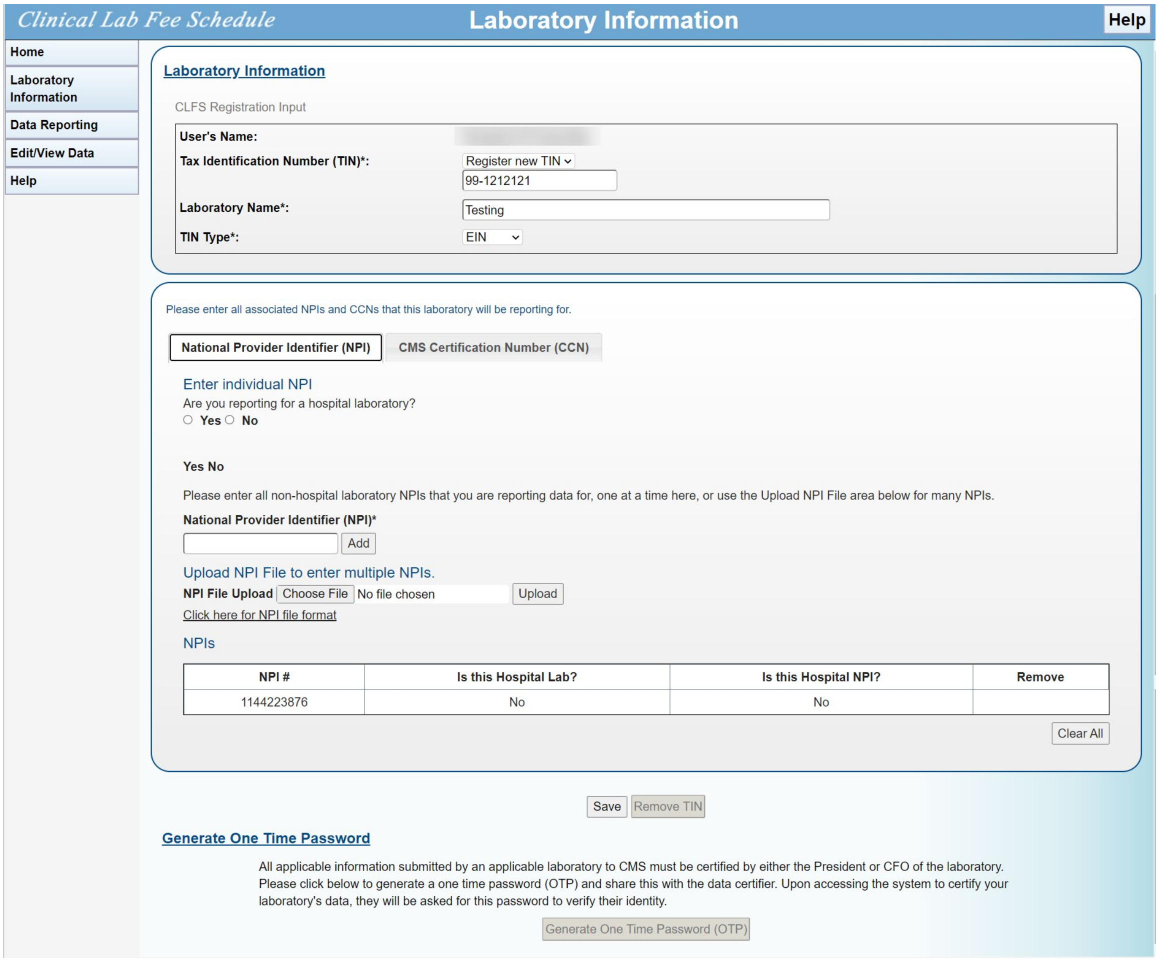
Generate One Time Password

All applicable information submitted by an applicable laboratory to CMS must be certified by either the President or CFO of the laboratory. Please click below to generate a one time password (OTP) and share this with the data certifier. Upon accessing the system to certify your laboratory's data, they will be asked for this password to verify their identity.

4. To register additional TINs, select “Register new TIN” from the TIN drop-down list, and enter a new TIN, Lab name, NPI(s) while answering the NPI question regarding Hospital Laboratories, and CCN(s).

   The data for the new TIN populates as shown in Figure 4-3.

Figure 4-3: Laboratory Information – Registering an Additional TIN



Laboratory Information

CLFS Registration Input

User's Name:	[redacted]
Tax Identification Number (TIN)*:	Register new TIN 99-1212121
Laboratory Name*:	Testing
TIN Type*:	EIN

Please enter all associated NPIs and CCNs that this laboratory will be reporting for.

National Provider Identifier (NPI) | CMS Certification Number (CCN)

Enter individual NPI

Are you reporting for a hospital laboratory?

○ Yes ○ No

Yes No

Please enter all non-hospital laboratory NPIs that you are reporting data for, one at a time here, or use the Upload NPI File area below for many NPIs.

National Provider Identifier (NPI)*

Add

Upload NPI File to enter multiple NPIs.

NPI File Upload Choose File No file chosen Upload

Click here for NPI file format

NPIs

NPI #	Is this Hospital Lab?	Is this Hospital NPI?	Remove
1144223876	No	No	

Clear All

Save Remove TIN

Generate One Time Password

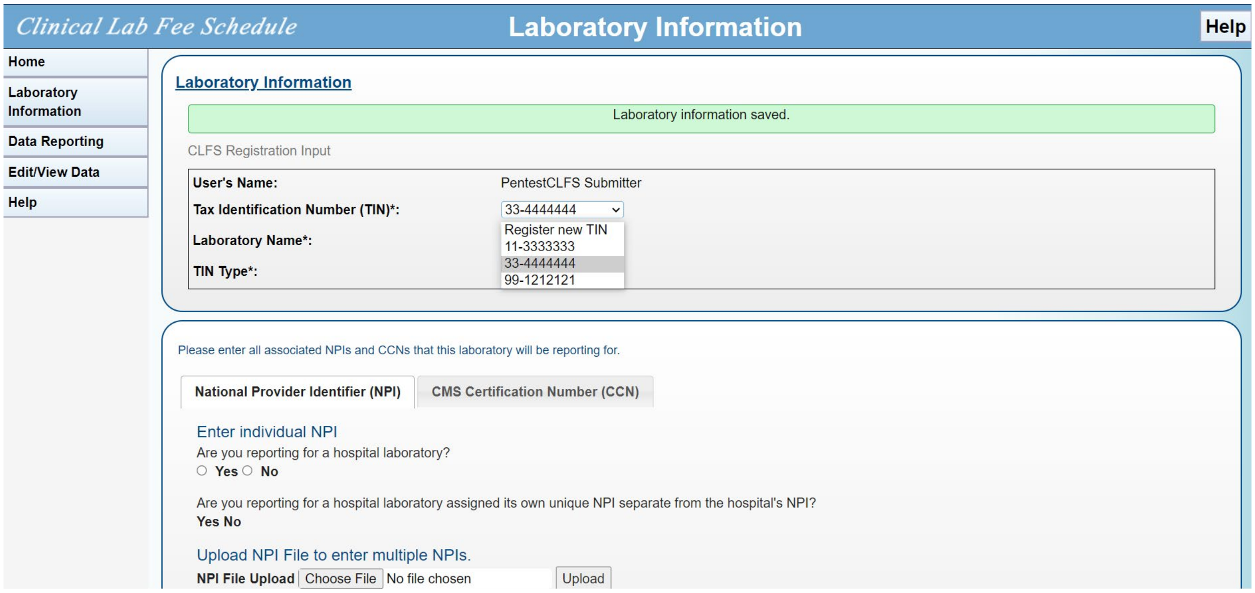
All applicable information submitted by an applicable laboratory to CMS must be certified by either the President or CFO of the laboratory. Please click below to generate a one time password (OTP) and share this with the data certifier. Upon accessing the system to certify your laboratory's data, they will be asked for this password to verify their identity.

Generate One Time Password (OTP)

5. Click on the **Save** button,

   A message displays that the laboratory information has been saved, and the drop-down list displays a list with the new TIN added, as shown in Figure 4-4.

Figure 4-4: Laboratory Information – Additional TIN Registered



Clinical Lab Fee Schedule
Laboratory Information
Help
Home
Laboratory Information
Data Reporting
Edit/View Data
Help

Laboratory Information

Laboratory information saved.

CLFS Registration Input

User's Name: PentestCLFS Submitter

Tax Identification Number (TIN)*: 33-4444444

Register new TIN
11-3333333
33-4444444
99-1212121

Laboratory Name*:

TIN Type*:

Please enter all associated NPIs and CCNs that this laboratory will be reporting for.

National Provider Identifier (NPI)
CMS Certification Number (CCN)

Enter individual NPI

Are you reporting for a hospital laboratory?

○ Yes ○ No

Are you reporting for a hospital laboratory assigned its own unique NPI separate from the hospital's NPI?

Yes No

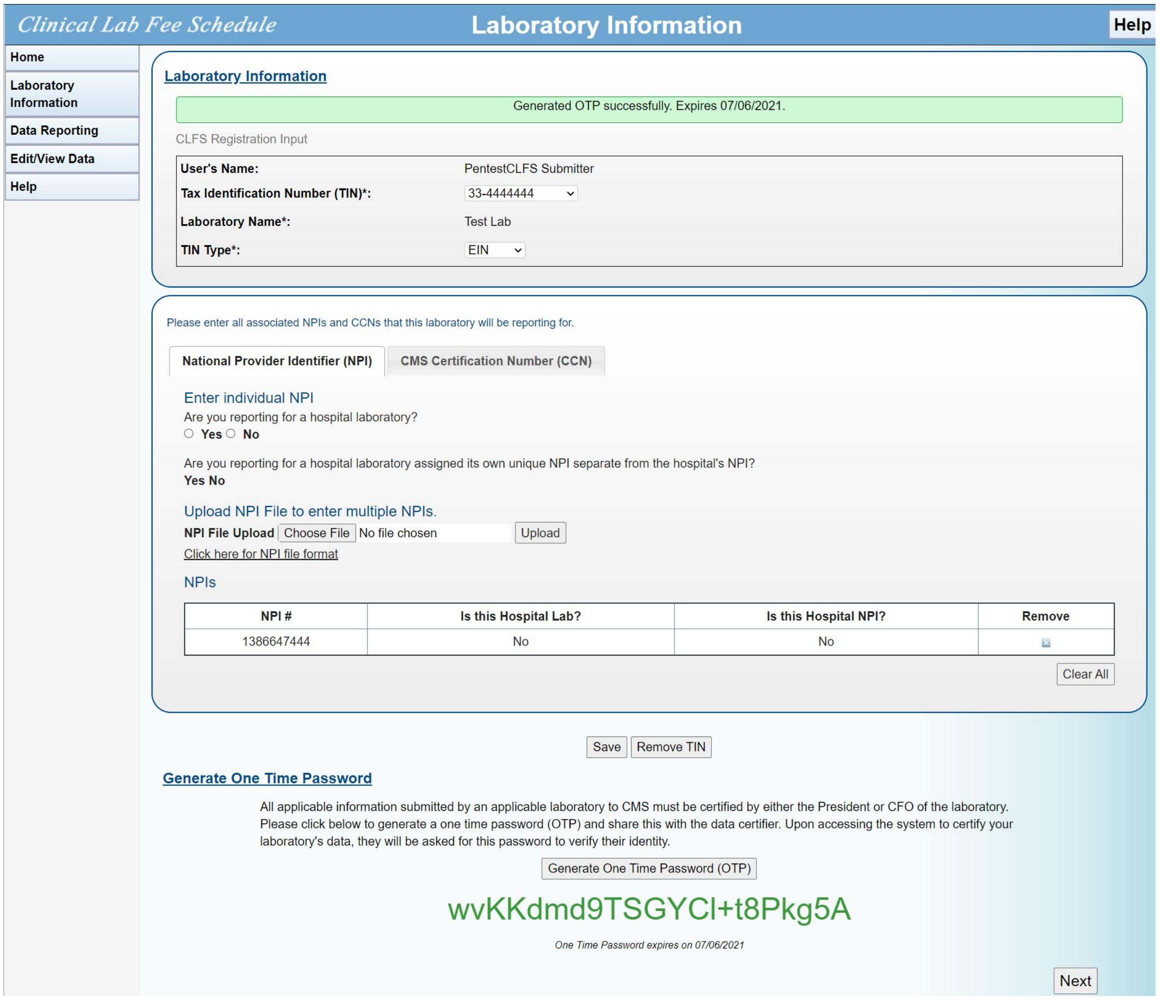
Upload NPI File to enter multiple NPIs.

NPI File Upload Choose File No file chosen Upload

6. When it is known who the CLFS Certifier for the same reporting TIN(s) will be, generate an OTP to provide to the CLFS Certifier in your organization to complete registration. This is done by clicking on the **Generate One Time Password (OTP)** button.

   The application displays the OTP, which will be valid for 7 days as shown in Figure 4-5.

Figure 4-5: Laboratory Information – Generated OTP Page


Clinical Lab Fee Schedule
Laboratory Information
Help
Home
Laboratory Information
Data Reporting
Edit/View Data
Help
Laboratory Information
National Provider Identifier (NPI)
CMS Certification Number (CCN)
Choose File
Upload
Click here for NPI file format
Clear All
Save
Remove TIN
Generate One Time Password
Generate One Time Password (OTP)
Next

Generated OTP successfully. Expires 07/06/2021.

CLFS Registration Input

User's Name:	PentestCLFS Submitter
Tax Identification Number (TIN)*:	33-4444444
Laboratory Name*:	Test Lab
TIN Type*:	EIN

Please enter all associated NPIs and CCNs that this laboratory will be reporting for.

Enter individual NPI

Are you reporting for a hospital laboratory?

○ **Yes** ○ **No**

Are you reporting for a hospital laboratory assigned its own unique NPI separate from the hospital's NPI?

Yes No

Upload NPI File to enter multiple NPIs.

NPI File Upload No file chosen

NPIs

NPI #	Is this Hospital Lab?	Is this Hospital NPI?	Remove
1386647444	No	No	

All applicable information submitted by an applicable laboratory to CMS must be certified by either the President or CFO of the laboratory. Please click below to generate a one time password (OTP) and share this with the data certifier. Upon accessing the system to certify your laboratory's data, they will be asked for this password to verify their identity.

wvKKdmd9TSGYCl+t8Pkg5A

One Time Password expires on 07/06/2021

7. Copy the OTP and share it to the person assigned to be the CLFS Certifier.

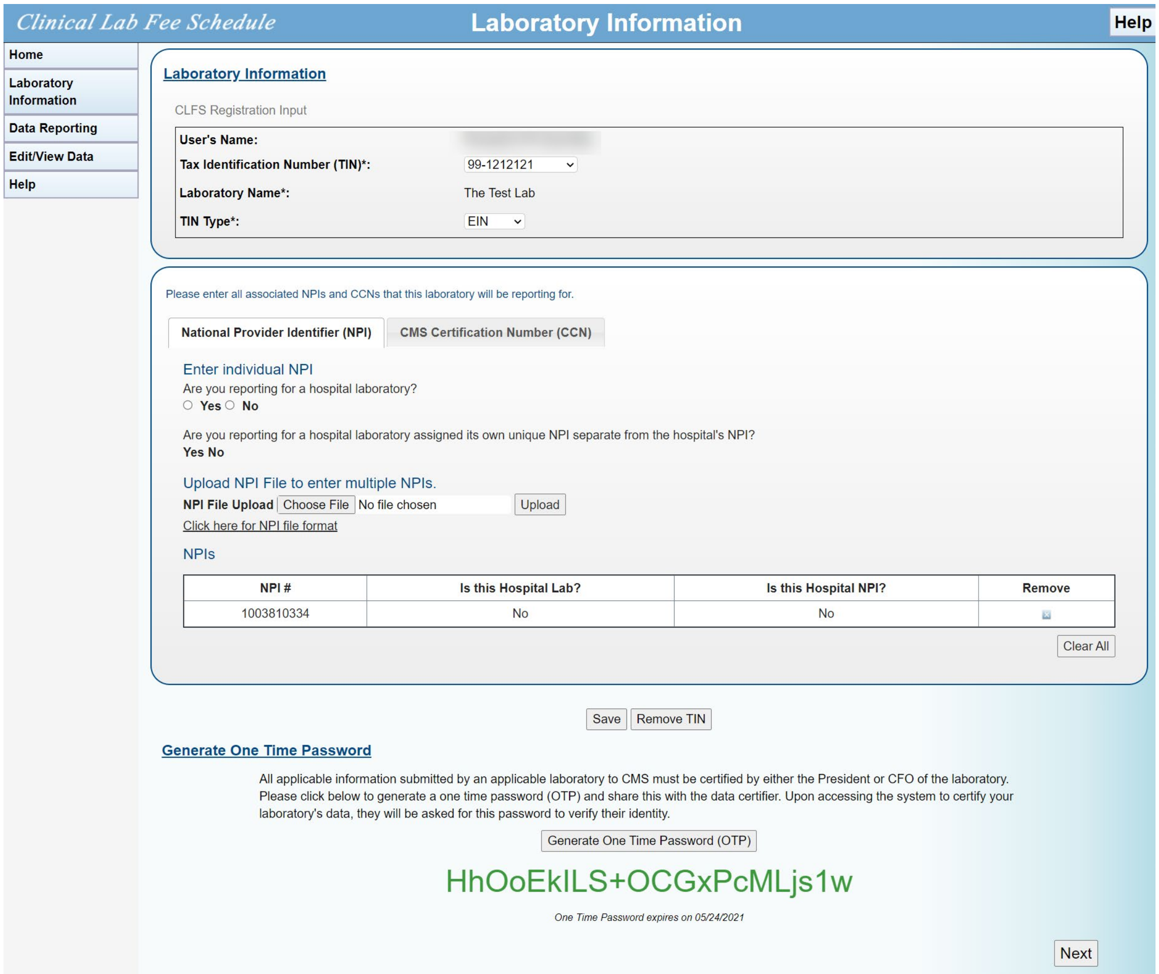
4.2 Remove Laboratory Information

If a user needs to remove an NPI or TIN from their profile, the following steps are to be used to as a CLFS Submitter:

1. Log in to CLFS as CLFS Submitter to open the “Laboratory Information” page.

   The “Laboratory Information” page displays as shown in Figure 4-6.

Figure 4-6: Laboratory Information Page



Laboratory Information

CLFS Registration Input

User's Name:	[redacted]
Tax Identification Number (TIN)*:	99-1212121
Laboratory Name*:	The Test Lab
TIN Type*:	EIN

Please enter all associated NPIs and CCNs that this laboratory will be reporting for.

National Provider Identifier (NPI) | CMS Certification Number (CCN)

Enter individual NPI

Are you reporting for a hospital laboratory?

○ **Yes** ○ **No**

Are you reporting for a hospital laboratory assigned its own unique NPI separate from the hospital's NPI?

Yes No

Upload NPI File to enter multiple NPIs.

NPI File Upload Choose File No file chosen Upload

Click here for NPI file format

NPIs

NPI #	Is this Hospital Lab?	Is this Hospital NPI?	Remove
1003810334	No	No	☒

Clear All

Save Remove TIN

Generate One Time Password

All applicable information submitted by an applicable laboratory to CMS must be certified by either the President or CFO of the laboratory. Please click below to generate a one time password (OTP) and share this with the data certifier. Upon accessing the system to certify your laboratory's data, they will be asked for this password to verify their identity.

Generate One Time Password (OTP)

HhOoEkILS+OCGxPcMLjs1w

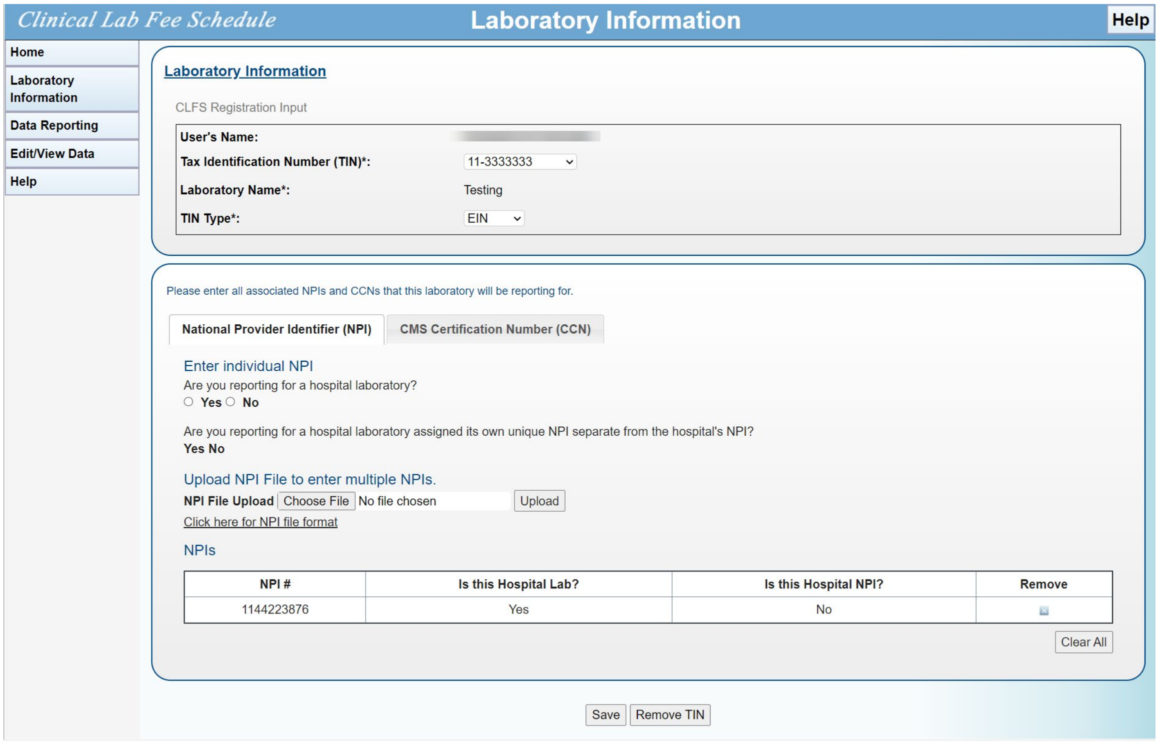
One Time Password expires on 05/24/2021

Next

2. To remove a TIN, select a TIN from the TIN drop-down list.

   The “Laboratory Information” page displays with the selected TIN to be removed, as shown in Figure 4-7.

Figure 4-7: Laboratory Information Page – TIN Selected


Clinical Lab Fee Schedule
Laboratory Information
Help
Home
Laboratory Information
Data Reporting
Edit/View Data
Help

Laboratory Information

CLFS Registration Input

User's Name:	[redacted]
Tax Identification Number (TIN)*:	11-3333333
Laboratory Name*:	Testing
TIN Type*:	EIN

Please enter all associated NPIs and CCNs that this laboratory will be reporting for.

National Provider Identifier (NPI)
CMS Certification Number (CCN)

Enter individual NPI

Are you reporting for a hospital laboratory?

○ Yes ○ No

Are you reporting for a hospital laboratory assigned its own unique NPI separate from the hospital's NPI?

Yes No

Upload NPI File to enter multiple NPIs.

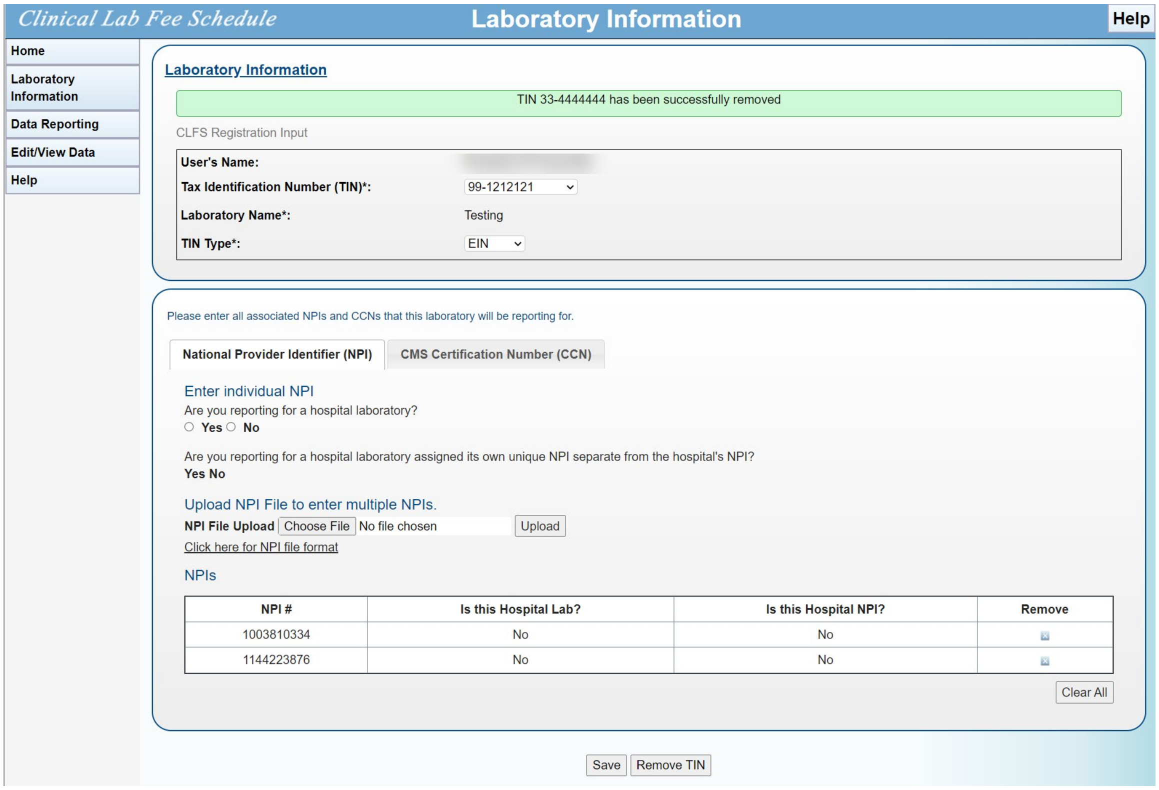
NPI File Upload Choose File No file chosen Upload

Click here for NPI file format

NPIs

NPI #	Is this Hospital Lab?	Is this Hospital NPI?	Remove
1144223876	Yes	No	☒

Figure 4-8: Laboratory Information – TIN Removed



Clinical Lab Fee Schedule
Laboratory Information
Help
Home
Laboratory Information
Data Reporting
Edit/View Data
Help

Laboratory Information

TIN 33-4444444 has been successfully removed

CLFS Registration Input

User's Name:	[redacted]
Tax Identification Number (TIN)*:	99-1212121
Laboratory Name*:	Testing
TIN Type*:	EIN

Please enter all associated NPIs and CCNs that this laboratory will be reporting for.

National Provider Identifier (NPI)
CMS Certification Number (CCN)

Enter individual NPI

Are you reporting for a hospital laboratory?

○ **Yes** ○ **No**

Are you reporting for a hospital laboratory assigned its own unique NPI separate from the hospital's NPI?

Yes No

Upload NPI File to enter multiple NPIs.

NPI File Upload Choose File No file chosen Upload

Click here for NPI file format

NPIs

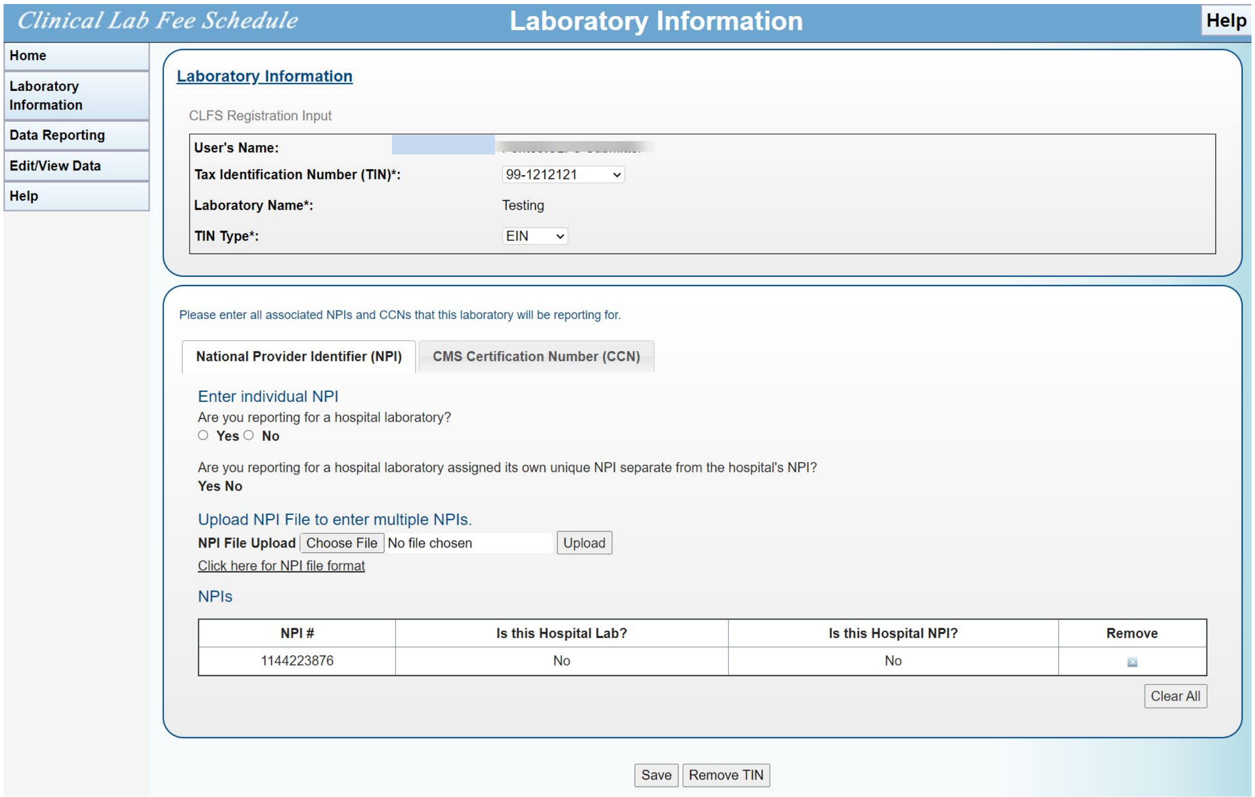
NPI #	Is this Hospital Lab?	Is this Hospital NPI?	Remove
1003810334	No	No	☒
1144223876	No	No	☒

3. To remove an NPI click the box under Remove.

   Note: At least one NPI must remain in the list.

   The list box refreshes and the selected NPI and/or CCN are removed from the list, as shown in Figure 4-9.

Figure 4-9: Removed NPI



Laboratory Information

CLFS Registration Input

User's Name:	[redacted]
Tax Identification Number (TIN)*:	99-1212121
Laboratory Name*:	Testing
TIN Type*:	EIN

Please enter all associated NPIs and CCNs that this laboratory will be reporting for.

National Provider Identifier (NPI) CMS Certification Number (CCN)

Enter individual NPI

Are you reporting for a hospital laboratory?
○ Yes ○ No

Are you reporting for a hospital laboratory assigned its own unique NPI separate from the hospital's NPI?
Yes No

Upload NPI File to enter multiple NPIs.

NPI File Upload Choose File No file chosen Upload

Click here for NPI file format

NPIs

NPI #	Is this Hospital Lab?	Is this Hospital NPI?	Remove
1144223876	No	No	

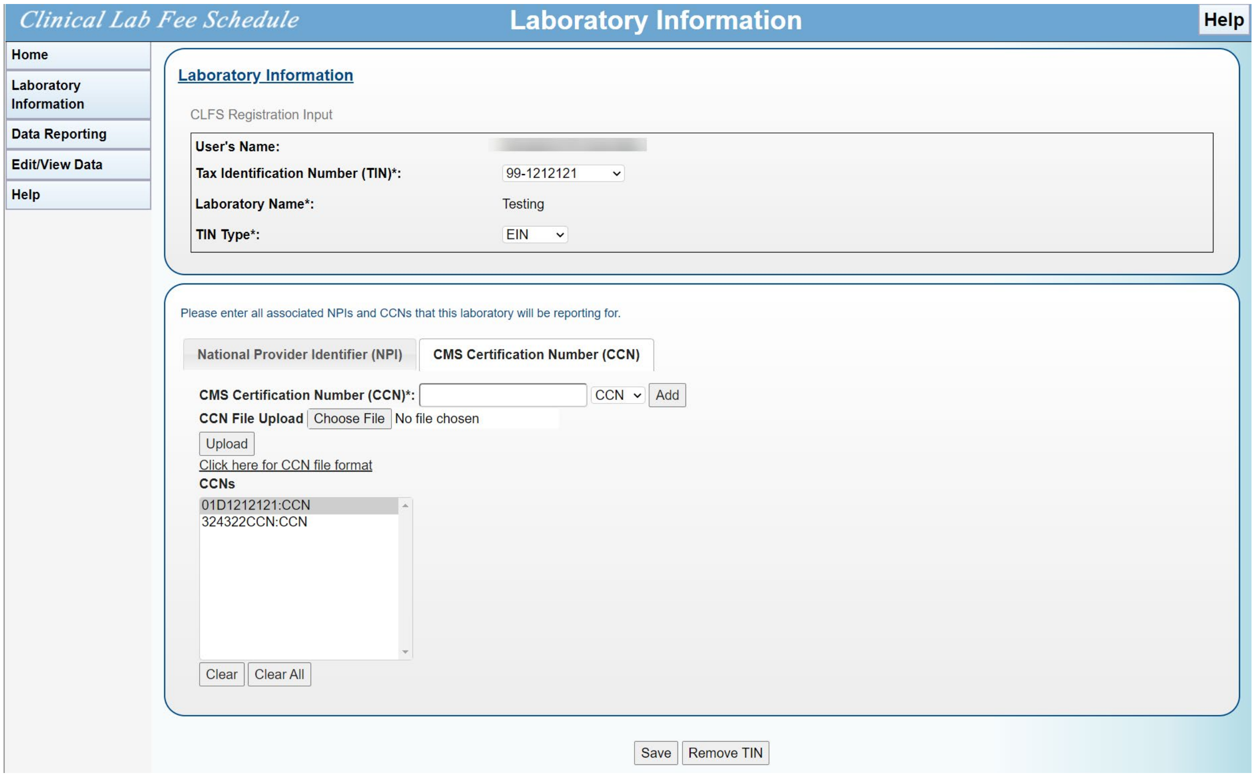
Clear All

Save Remove TIN

4. To remove a CCN, click on the CMS Certification Number (CCN) tab and select the CCN to be removed from the list box then click the Clear button.

   Note: At least one CCN must remain in the list.

Figure 4-10: Laboratory Information with Selected CCN



Laboratory Information

Laboratory Information

CLFS Registration Input

User's Name:	[redacted]
Tax Identification Number (TIN)*:	99-1212121
Laboratory Name*:	Testing
TIN Type*:	EIN

Please enter all associated NPIs and CCNs that this laboratory will be reporting for.

CMS Certification Number (CCN)*: CCN

CCN File Upload No file chosen

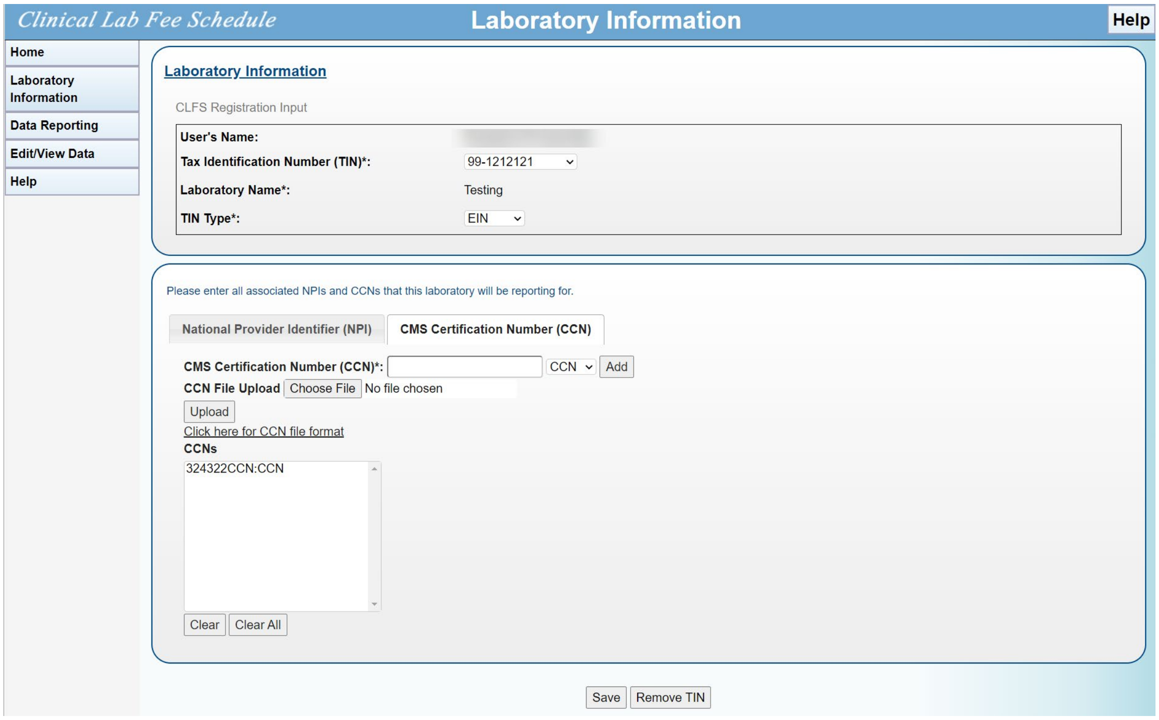
Click here for CCN file format

CCNs

01D1212121:CCN
324322CCN:CCN

5. The list box refreshes and the selected CCN is removed from the list, as shown in Figure 4-11.
6. Click on the **Save** button.

Figure 4-111: Laboratory Information with Selected CCN Removed



CLFS Registration Input

User's Name:	[redacted]
Tax Identification Number (TIN)*:	99-1212121
Laboratory Name*:	Testing
TIN Type*:	EIN

Please enter all associated NPIs and CCNs that this laboratory will be reporting for.

CMS Certification Number (CCN)*:

CCN File Upload No file chosen

CCNs

324322CCN:CCN

5. Data Reporting

Applicable laboratories are required to report applicable information to the CLFS application using a file upload or through manual online data entry. The following sections detail the steps required to submit applicable laboratory data using file uploads and manual online data entry.

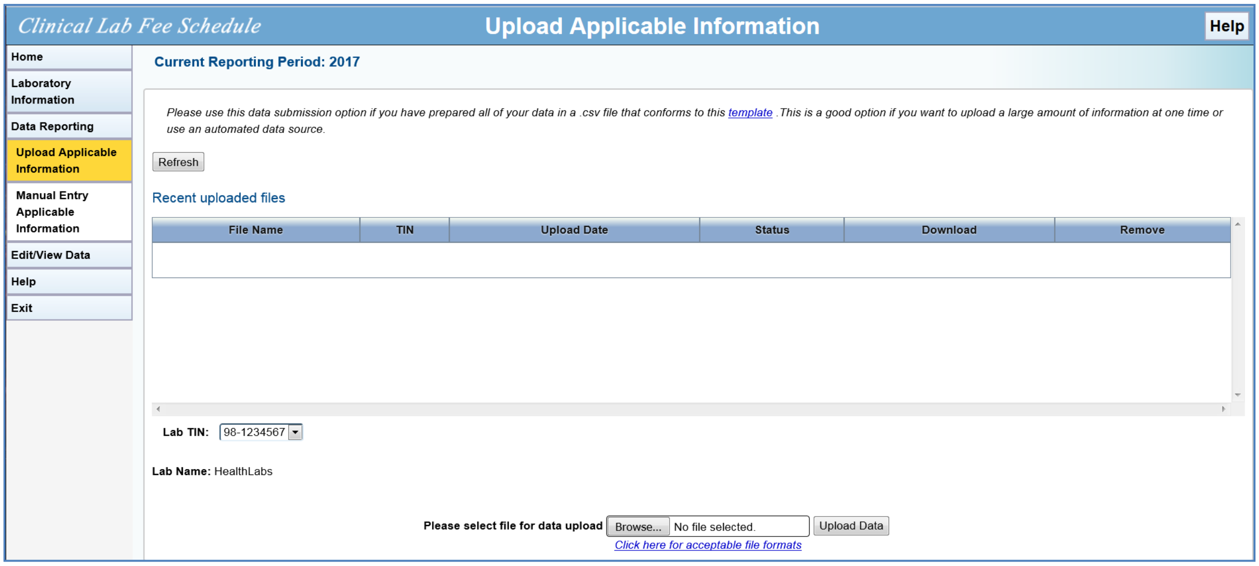
5.1 Upload Applicable Information - CLFS Submitter

The CLFS application provides applicable laboratories the ability to report applicable information to CMS using a file upload. Perform the following steps to enter data using the upload process:

1. Log in as CLFS Submitter and click on **Data Reporting** and then click on **Upload Applicable Information**.

   The "Upload Applicable Information" page displays as shown in Figure 5-1.

Figure 5-1: Upload Applicable Information Page



Clinical Lab Fee Schedule
Upload Applicable Information
Help
Home
Laboratory Information
Data Reporting
Upload Applicable Information
Manual Entry Applicable Information
Edit/View Data
Help
Exit

Current Reporting Period: 2017

Please use this data submission option if you have prepared all of your data in a .csv file that conforms to this template . This is a good option if you want to upload a large amount of information at one time or use an automated data source.

Recent uploaded files

File Name	TIN	Upload Date	Status	Download	Remove

Lab TIN: 98-1234567

Lab Name: HealthLabs

Please select file for data upload Browse... No file selected.

At the top center of the page is a link to the data reporting template that could be used to enter data in .csv format. Previous upload submissions will be displayed at the upper portion of the page. Only one file per TIN can be uploaded (one file can include all NPIs under each TIN).

Note: Template Requirements

- You may change the filename
- Do not add additional columns to the template
- Do not add, remove, or otherwise change columns or column headings within the template
- Do not submit blank rows between data entries
- You must submit all data in contiguous rows
- Enter the HCPCS Code, Payment Rate, Volume, and NPI. The basic edits for the data items are:

a. HCPCS Code: alphanumeric or all numeric
5 characters

b. Payment Rate: numeric
not a negative value
999.99 format
Checked against current CLFS rate; a warning will appear if payment rate entered is greater than (10,000%) above National rate. Payment rate is defined as the rate per test.

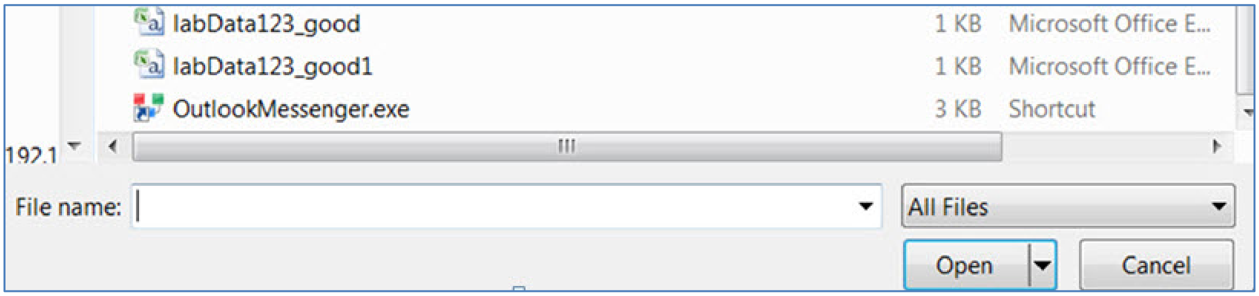
c. Volume: numeric
not a negative value
can be zero
no decimal places

d. NPI: numeric
10 digits fixed
no decimal places
cannot have 5 consecutive same digits
must pass Luhn check digit formula

2. To upload the data, click on the **Browse…** button.

   The file directory window displays as shown in Figure 5-2.

Figure 5-2: File Directory Window



labData123_good	1 KB	Microsoft Office E...
labData123_good1	1 KB	Microsoft Office E...
OutlookMessenger.exe	3 KB	Shortcut

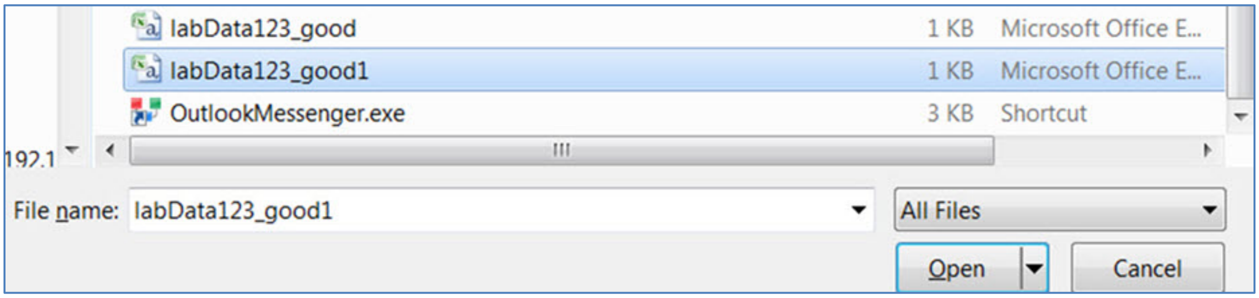
File name:

All Files

3. Select the directory path and filename to upload.

   The filename appears in the “File name” window as shown in Figure 5-3.

Figure 5-3: Filename Window



labData123_good	1 KB	Microsoft Office E...
labData123_good1	1 KB	Microsoft Office E...
OutlookMessenger.exe	3 KB	Shortcut

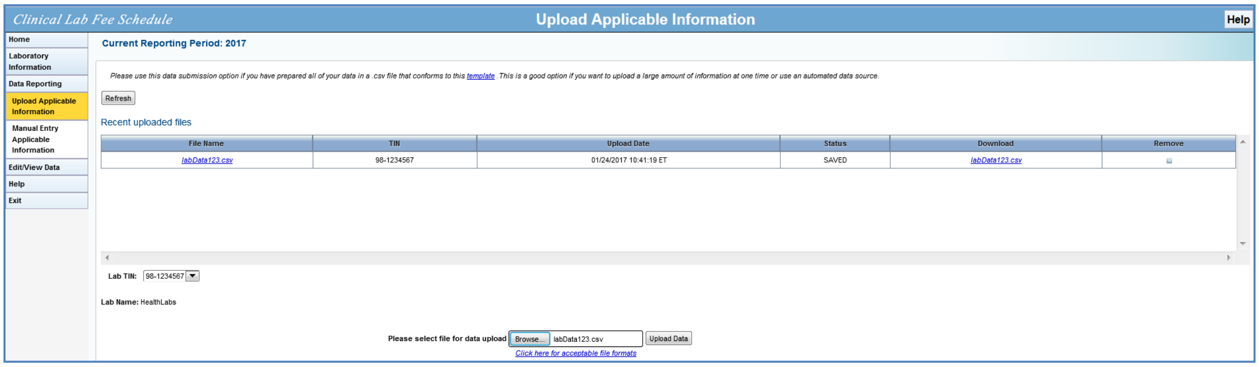
File name: labData123_good1

All Files

4. Click on the **Open** button.

   The filename appears in the “Browse” window as shown in Figure 5-4.

Figure 5-4: Browse Window



Clinical Lab Fee Schedule
Upload Applicable Information
Help
Home
Laboratory Information
Data Reporting
Upload Applicable Information
Manual Entry Applicable Information
Edit/View Data
Help
Exit
Refresh
Browse...
Upload Data

Current Reporting Period: 2017

Please use this data submission option if you have prepared all of your data in a .csv file that conforms to this template . This is a good option if you want to upload a large amount of information at one time or use an automated data source.

Recent uploaded files

File Name	TIN	Upload Date	Status	Download	Remove
labData123.csv	98-1234567	01/24/2017 10:41:19 ET	SAVED	labData123.csv	□

Lab TIN: 98-1234567

Lab Name: HealthLabs

Please select file for data upload labData123.csv

Click here for acceptable file formats

5. Click on the **Upload Data** button.

   The **Refresh** button can be clicked when an upload is taking a while to process to see if the upload is still processing or completed. Multiple uploads are allowed. Duplicate data is also allowed if applicable, please use caution to ensure that all data that appears to be duplicated is legitimate. After the upload process has completed, the results will be displayed at the bottom of the screen.

   Note: If the status returns a result of “ERROR,” click on the link in the “Filename” column to receive the description of the error in your database.

   Note:

   - If the file being uploaded is greater than 3,400,183 bytes, but less than 29,360,128 bytes, it is considered a Large Volume (LV) file. Once an LV file is uploaded your role will be modified to an LV Submitter. For further instructions on how to Upload, Edit, or Delete data for LV files, please refer to sections 5.2 and 5.2.1.

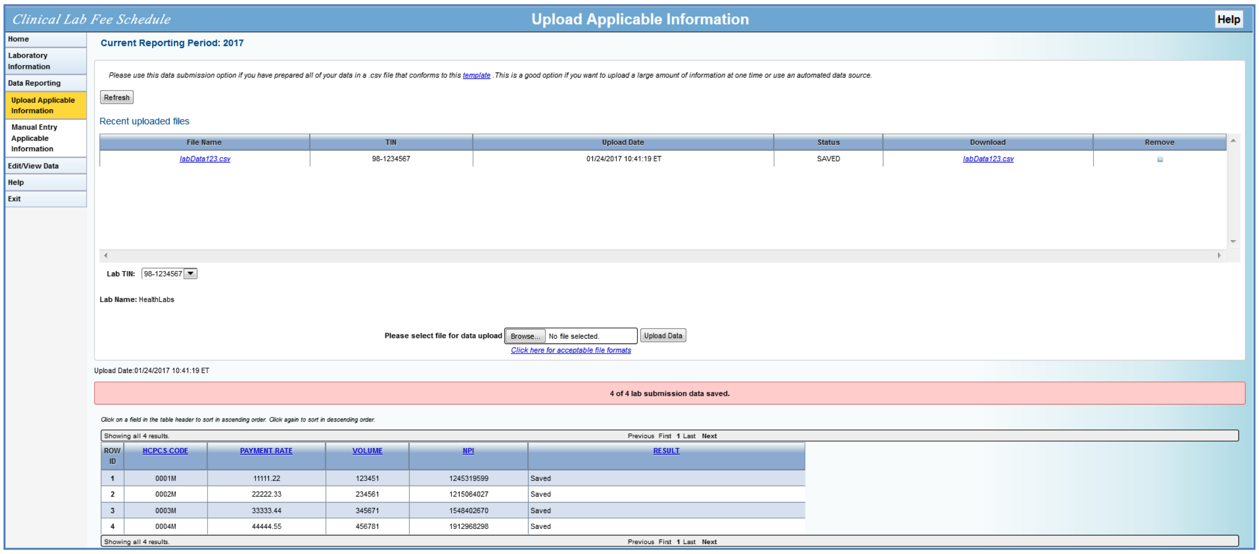
     A message will display stating “A Large Volume file is detected and will be submitted tonight after business hours. The results of this upload will be available tomorrow, please review the results then.”

   - If the file being uploaded is greater than 29,360,128 bytes, it is considered a Very Large Volume (VLV) file. Once a VLV file is uploaded your role will be modified to a VLV Submitter. For further instructions on how to Upload, Edit, or Delete data for VLV files, please refer to sections 0 and 5.3.1.

     A message will display stating “A Very Large Volume file is detected and will be submitted tonight after business hours. The results of this upload will be available tomorrow, please review the results then.”

   The data from the uploaded data template displays on the screen as shown in Figure 5-5.

Figure 5-5: Uploaded Data Page - Normal


Clinical Lab Fee Schedule
Help
Home
Laboratory Information
Data Reporting
Upload Applicable Information
Manual Entry Applicable Information
Edit/View Data
Help
Exit
Refresh
Browse...
Upload Data
Previous First 1 Last Next

Upload Applicable Information

Current Reporting Period: 2017

Please use this data submission option if you have prepared all of your data in a .csv file that conforms to this template. This is a good option if you want to upload a large amount of information at one time or use an automated data source.

Recent uploaded files

File Name	TIN	Upload Date	Status	Download	Remove
labData123.csv	98-1234567	01/24/2017 10:41:19 ET	SAVED	labData123.csv	☐

Lab TIN: 98-1234567

Lab Name: HealthLabs

Please select file for data upload: No file selected.

Click here for acceptable file formats

Upload Date:01/24/2017 10:41:19 ET

4 of 4 lab submission data saved.

Click on a field in the table header to sort in ascending order. Click again to sort in descending order.

Showing all 4 results.

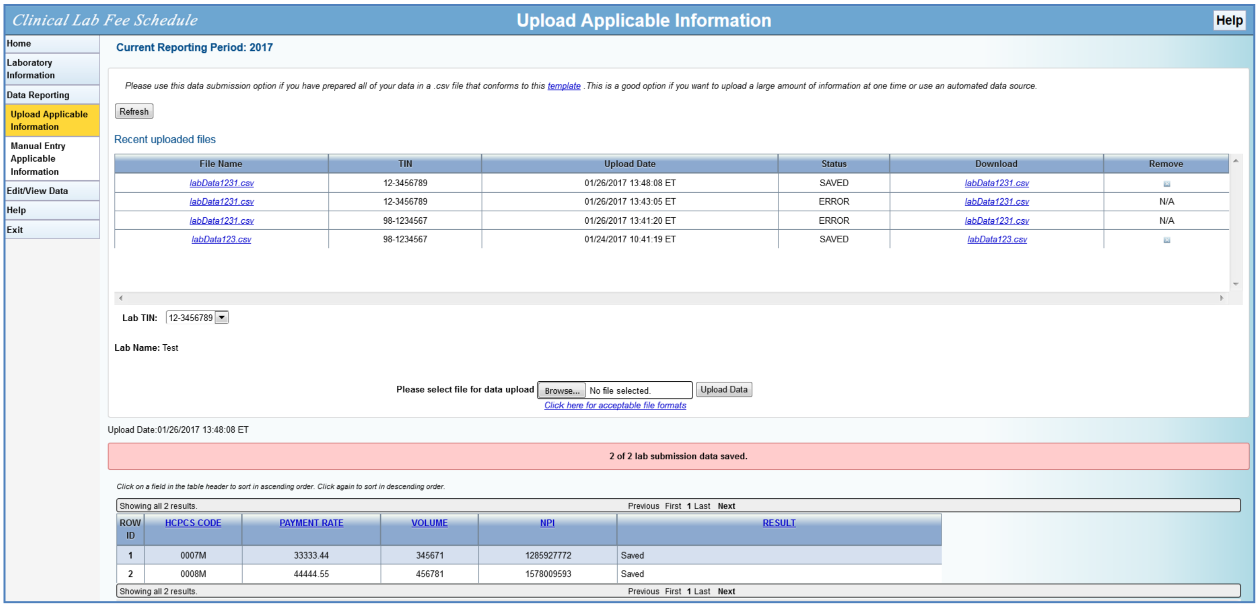
ROW ID	HCPCS CODE	PAYMENT RATE	VOLUME	NPI	RESULT
1	0001M	11111.22	123451	1245319599	Saved
2	0002M	22222.33	234561	1215064027	Saved
3	0003M	33333.44	345671	1548402670	Saved
4	0004M	44444.55	456781	1912968298	Saved

Showing all 4 results.

Data can be sorted in HCPCS code order in ascending or descending order as well as the “NPI” and “Result” fields (can be used when locating errors). The data can be viewed using the scroll features. If there is at least one validation error on the entire file, none of the data are saved. The data are only saved when the entire file has no validation errors. The “Result” field will give the details of the data validation errors(s). All the records that pass validation will have the message *# of # lab submission data saved*. In the “Result” field, when all the data have passed validation, each entry will have the message *Saved*.

6. To remove an uploaded and saved file, click on the box in the “Removed” column, as shown in Figure 5-6.

Figure 5-6: Uploaded Applicable Information – Data Removal


Clinical Lab Fee Schedule
Help
Home
Laboratory Information
Data Reporting
Upload Applicable Information
Manual Entry Applicable Information
Edit/View Data
Help
Exit
Refresh
Browse...
Upload Data
Previous First 1 Last Next

Upload Applicable Information

Current Reporting Period: 2017

Please use this data submission option if you have prepared all of your data in a .csv file that conforms to this template. This is a good option if you want to upload a large amount of information at one time or use an automated data source.

Recent uploaded files

File Name	TIN	Upload Date	Status	Download	Remove
labData1231.csv	12-3456789	01/26/2017 13:48:08 ET	SAVED	labData1231.csv	☐
labData1231.csv	12-3456789	01/26/2017 13:43:05 ET	ERROR	labData1231.csv	N/A
labData1231.csv	98-1234567	01/26/2017 13:41:20 ET	ERROR	labData1231.csv	N/A
labData123.csv	98-1234567	01/24/2017 10:41:19 ET	SAVED	labData123.csv	☐

Lab TIN: 12-3456789

Lab Name: Test

Please select file for data upload: No file selected.

Click here for acceptable file formats

Upload Date:01/26/2017 13:48:08 ET

2 of 2 lab submission data saved.

Click on a field in the table header to sort in ascending order. Click again to sort in descending order.

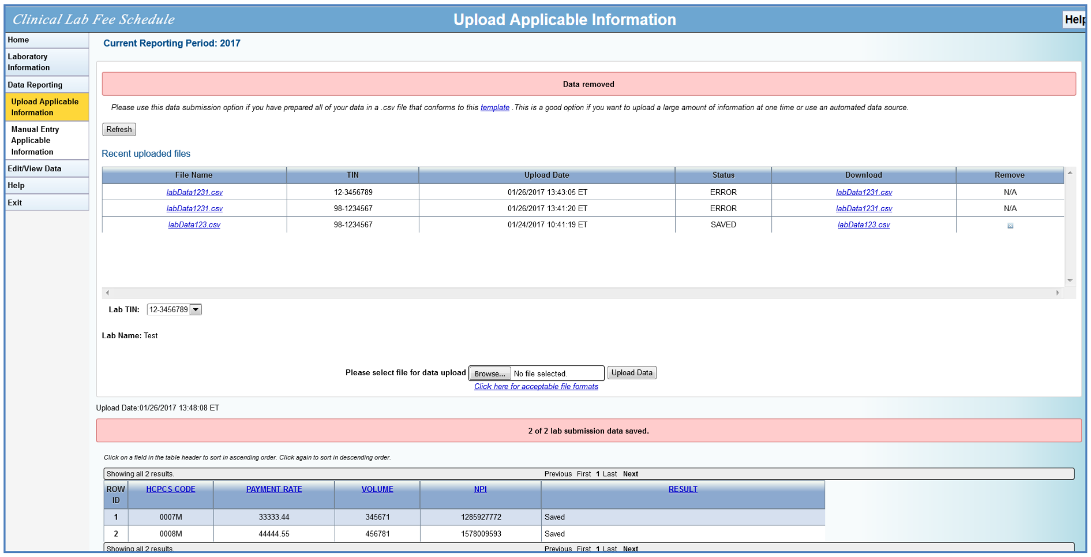
Showing all 2 results.

ROW ID	HCPCS CODE	PAYMENT RATE	VOLUME	NPI	RESULT
1	0007M	33333.44	345671	1285927772	Saved
2	0008M	44444.55	456781	1578009593	Saved

Showing all 2 results.

7. The selected file to be removed automatically disappears from the list and a message displays stating that the data have been removed, as shown in Figure 5-7.

Figure 5-7: Uploaded Applicable Information – Data Removed


Clinical Lab Fee Schedule
Upload Applicable Information
Help
Home
Laboratory Information
Data Reporting
Upload Applicable Information
Manual Entry Applicable Information
Edit/View Data
Help
Exit

Current Reporting Period: 2017

Data removed

Please use this data submission option if you have prepared all of your data in a .csv file that conforms to this template . This is a good option if you want to upload a large amount of information at one time or use an automated data source.

Refresh

Recent uploaded files

File Name	TIN	Upload Date	Status	Download	Remove
labData1231.csv	12-3456789	01/26/2017 13:43:05 ET	ERROR	labData1231.csv	N/A
labData1231.csv	98-1234567	01/26/2017 13:41:20 ET	ERROR	labData1231.csv	N/A
labData123.csv	98-1234567	01/24/2017 10:41:19 ET	SAVED	labData123.csv	

Lab TIN: 12-3456789

Lab Name: Test

Please select file for data upload Browse... No file selected. Upload Data

Click here for acceptable file formats

Upload Date:01/26/2017 13:48:08 ET

2 of 2 lab submission data saved.

Click on a field in the table header to sort in ascending order. Click again to sort in descending order.

Showing all 2 results. Previous First **1** Last **Next**

ROW ID	HCPCS CODE	PAYMENT RATE	VOLUME	NPI	RESULT
1	0007M	33333.44	345671	1285927772	Saved
2	0008M	44444.55	456781	1578009593	Saved

Showing all 2 results. Previous First **1** Last **Next**

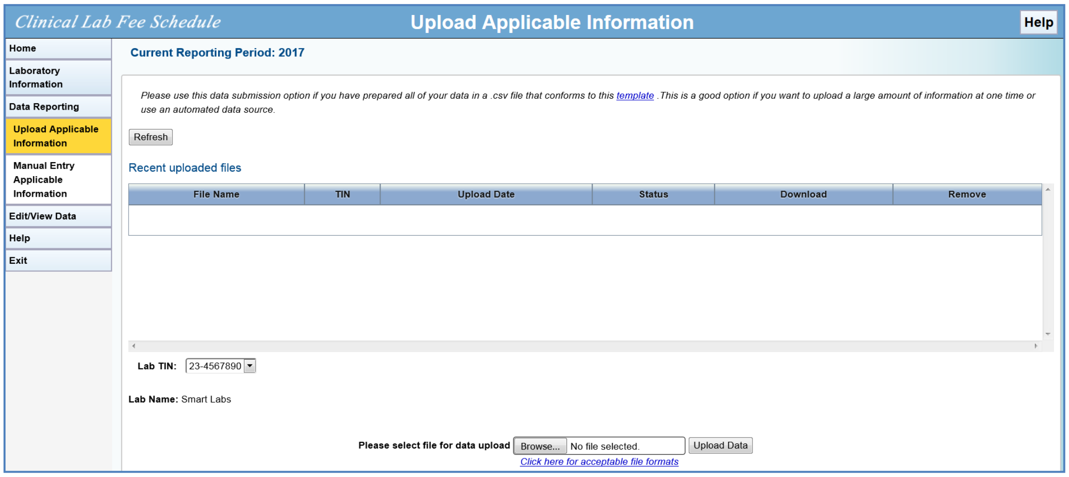
5.2 Upload Applicable Information – CLFS Submitter Large Volume (LV) Role

The CLFS application provides applicable laboratories the ability to report applicable information to CMS using a file transfer process. If the file being uploaded is greater than 3,400,183 bytes, but less than 29,360,128 bytes, it is considered an LV file. Once an LV file is uploaded your role will be modified to a LV Submitter. Perform the following steps to enter data using the upload process:

1. Log in as CLFS Submitter and click on **Data Reporting** and then click on **Upload Applicable Information**.

   The "Upload Applicable Information" page displays as shown in Figure 5-8.

Figure 5-8: Upload Applicable Information Page - LV


Clinical Lab Fee Schedule
Upload Applicable Information
Help
Home
Laboratory Information
Data Reporting
Upload Applicable Information
Manual Entry Applicable Information
Edit/View Data
Help
Exit

Current Reporting Period: 2017

Please use this data submission option if you have prepared all of your data in a .csv file that conforms to this template . This is a good option if you want to upload a large amount of information at one time or use an automated data source.

Refresh

Recent uploaded files

File Name	TIN	Upload Date	Status	Download	Remove

Lab TIN: 23-4567890

Lab Name: Smart Labs

Please select file for data upload Browse... No file selected. Upload Data

Click here for acceptable file formats

At the top center of the page is a link to the data reporting template that could be used to enter data in .csv format. Previous upload submissions will be displayed at the upper portion of the page.

Note: Template Requirements

- You may change the filename
- Do not add additional columns to the template
- Do not add, remove, or otherwise change columns or column headings within the template
- Do not submit blank rows between data entries
- You must submit all data in contiguous rows
- Enter the HCPCS Code, Payment Rate, Volume, and NPI. The basic edits for the data items are:

  a. HCPCS Code: alphanumeric or all numeric
  5 characters

  b. Payment Rate: numeric
  not a negative value
  999.99 format
  Checked against current CLFS rate; a warning will appear if payment rate entered is greater than (10,000%) above National rate. Payment rate is defined as the rate per test.

  c. Volume: numeric
  not a negative value
  can be zero
  no decimal places
  up to 6 digits

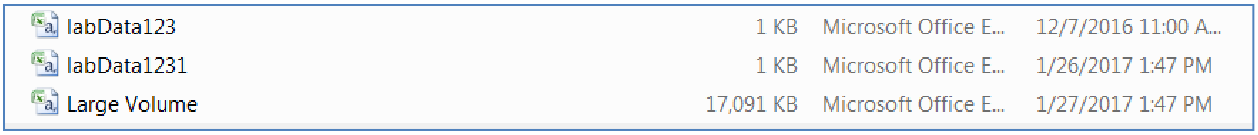
  d. NPI: numeric
  10 digits fixed
  no decimal places
  cannot have 5 consecutive same digits
  must pass Luhn check digit formula

The **Refresh** button is used when a submission is taking an extended period of time to process. By clicking on the **Refresh** button, the Submitter can see if the file upload is still processing or completed.

2. To upload the data, click on the **Browse…** button.

   The file directory window displays as shown in Figure 5-9.

Figure 5-9: File Directory Window - LV

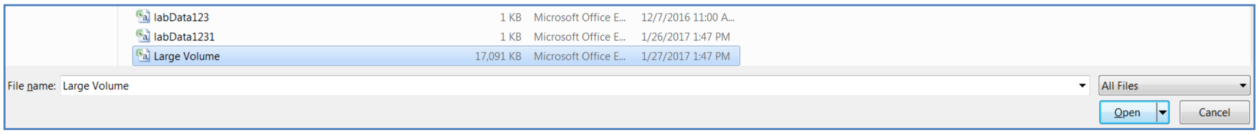


labData123	1 KB	Microsoft Office E...	12/7/2016 11:00 A...
labData1231	1 KB	Microsoft Office E...	1/26/2017 1:47 PM
Large Volume	17,091 KB	Microsoft Office E...	1/27/2017 1:47 PM

3. Select the directory path and filename to upload.

   The filename appears in the “File name” window as shown in Figure 5-10.

Figure 5-10: Filename Window - LV



labData123	1 KB	Microsoft Office E...	12/7/2016 11:00 A...
labData1231	1 KB	Microsoft Office E...	1/26/2017 1:47 PM
Large Volume	17,091 KB	Microsoft Office E...	1/27/2017 1:47 PM

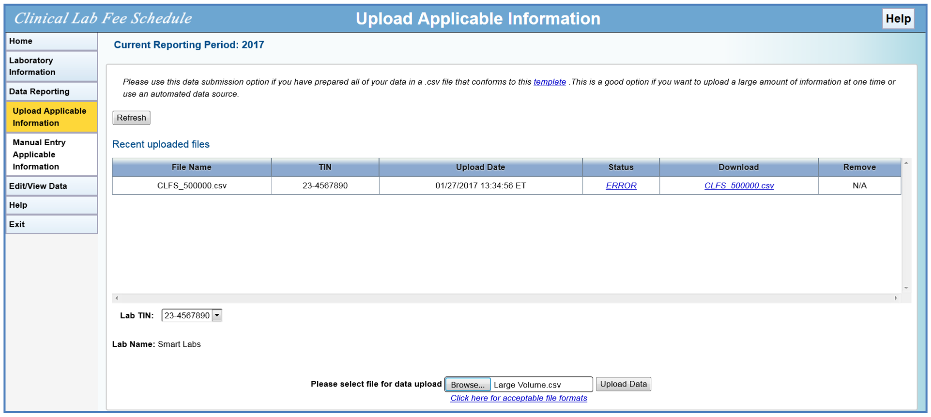
File name: Large Volume

All Files

4. Click on the **Open** button.

   The filename appears in the “Browse” window as shown in Figure 5-11.

Figure 5-11: Browse Window - LV



Clinical Lab Fee Schedule
Upload Applicable Information
Help
Home
Laboratory Information
Data Reporting
Upload Applicable Information
Manual Entry Applicable Information
Edit/View Data
Help
Exit
Refresh
Browse...
Upload Data

Current Reporting Period: 2017

Please use this data submission option if you have prepared all of your data in a .csv file that conforms to this template . This is a good option if you want to upload a large amount of information at one time or use an automated data source.

Recent uploaded files

File Name	TIN	Upload Date	Status	Download	Remove
CLFS_500000.csv	23-4567890	01/27/2017 13:34:56 ET	*ERROR*	*CLFS_500000.csv*	N/A

Lab TIN: 23-4567890

Lab Name: Smart Labs

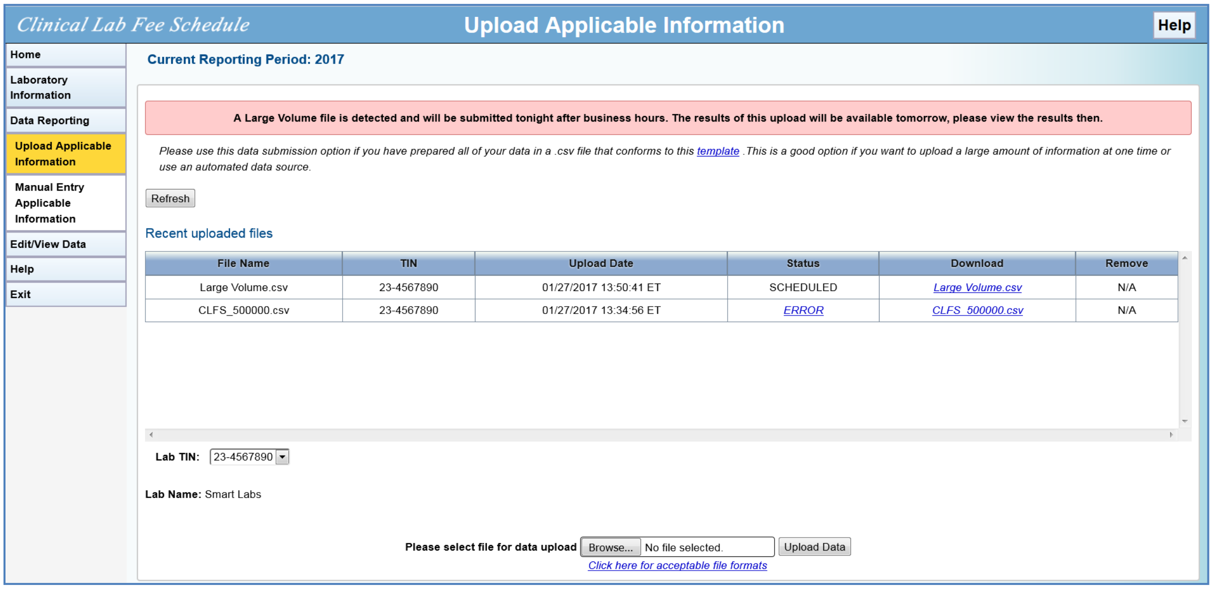
Please select file for data upload Large Volume.csv

Click here for acceptable file formats

5. Click on the **Upload Data** button.

   The file to upload displays with the Status as “Scheduled” and a message displays stating that an LV file has been detected and will be available tomorrow, as shown in Figure 5-12.

Figure 5-12: Large Volume Message Display



Clinical Lab Fee Schedule
Upload Applicable Information
Help
Home
Laboratory Information
Data Reporting
Upload Applicable Information
Manual Entry Applicable Information
Edit/View Data
Help
Exit
Refresh
Browse...
Upload Data

Current Reporting Period: 2017

A Large Volume file is detected and will be submitted tonight after business hours. The results of this upload will be available tomorrow, please view the results then.

Please use this data submission option if you have prepared all of your data in a .csv file that conforms to this template . This is a good option if you want to upload a large amount of information at one time or use an automated data source.

Recent uploaded files

File Name	TIN	Upload Date	Status	Download	Remove
Large Volume.csv	23-4567890	01/27/2017 13:50:41 ET	SCHEDULED	*Large Volume.csv*	N/A
CLFS_500000.csv	23-4567890	01/27/2017 13:34:56 ET	*ERROR*	*CLFS_500000.csv*	N/A

Lab TIN: 23-4567890

Lab Name: Smart Labs

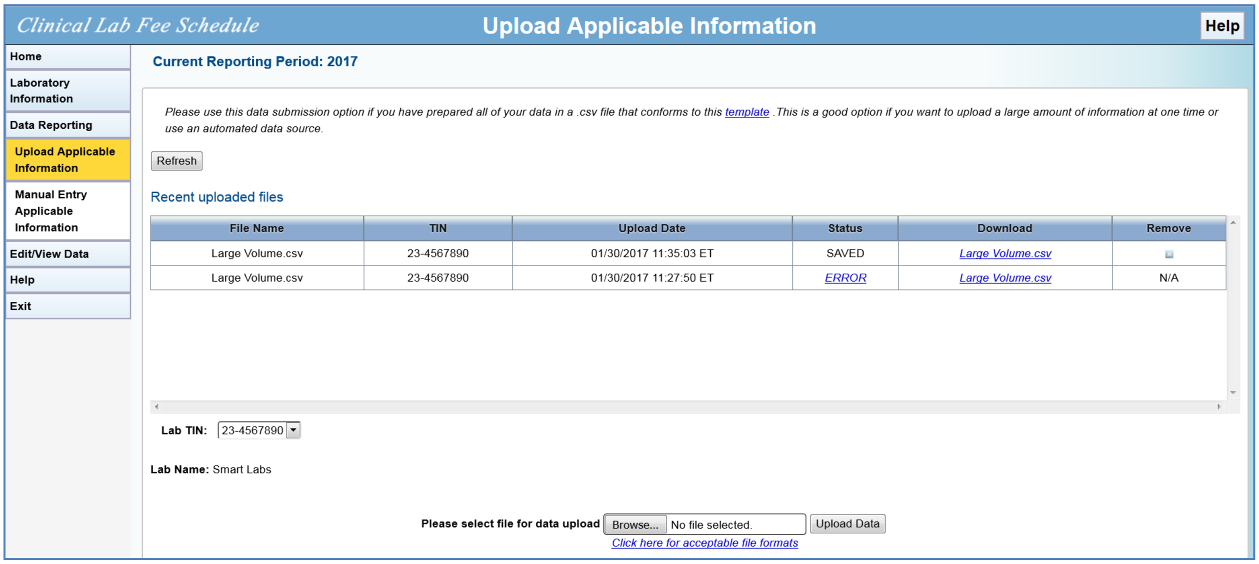
Please select file for data upload No file selected.

Click here for acceptable file formats

6. To know when the file has been saved, click on the **Refresh** button.

   The file to upload displays with the status as “SAVED” as shown in Figure 5-13.

Figure 5-13: Large Volume Data Saved


Clinical Lab Fee Schedule
Upload Applicable Information
Help
Home
Laboratory Information
Data Reporting
Upload Applicable Information
Manual Entry Applicable Information
Edit/View Data
Help
Exit
Refresh
Browse...
Upload Data

Current Reporting Period: 2017

Please use this data submission option if you have prepared all of your data in a .csv file that conforms to this template . This is a good option if you want to upload a large amount of information at one time or use an automated data source.

Recent uploaded files

File Name	TIN	Upload Date	Status	Download	Remove
Large Volume.csv	23-4567890	01/30/2017 11:35:03 ET	SAVED	Large Volume.csv	
Large Volume.csv	23-4567890	01/30/2017 11:27:50 ET	ERROR	Large Volume.csv	N/A

Lab TIN: 23-4567890

Lab Name: Smart Labs

Please select file for data upload No file selected.

Click here for acceptable file formats

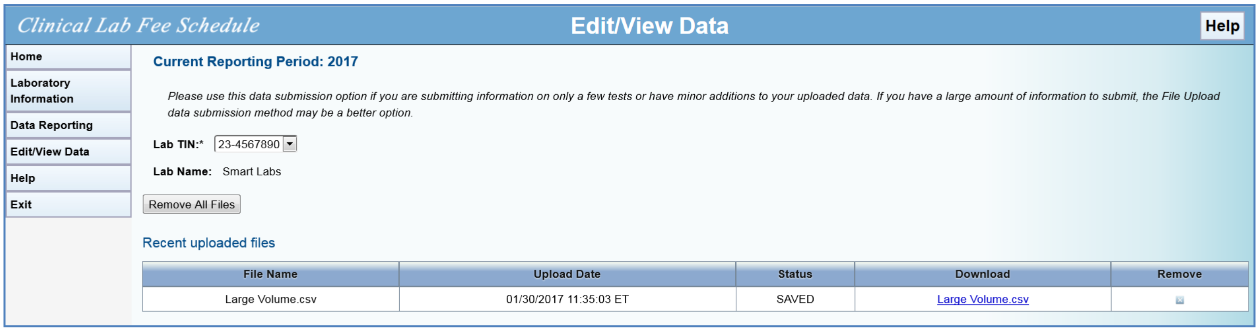
5.2.1 Edit/View Data – CLFS Submitter Large Volume Role

The CLFS application provides applicable laboratories the ability to edit information to CMS. Perform the following steps to edit data.

1. Log in as CLFS Submitter and click on **Edit/View Data**.

   The “Edit/View Data” window displays as shown in Figure 5-14.

Figure 5-14: Large Volume Edit/View Page



Current Reporting Period: 2017

Please use this data submission option if you are submitting information on only a few tests or have minor additions to your uploaded data. If you have a large amount of information to submit, the File Upload data submission method may be a better option.

Lab TIN:* 23-4567890

Lab Name: Smart Labs

Recent uploaded files

File Name	Upload Date	Status	Download	Remove
Large Volume.csv	01/30/2017 11:35:03 ET	SAVED	Large Volume.csv	

2. To edit data, click the file link in the “Download” section, and edit change the information in the .csv file. The basic edits for the data items are:

   a. HCPCS Code: alphanumeric or all numeric
      5 characters

   b. Payment Rate: numeric
      not a negative value
      999.99 format

Checked against current CLFS rate; a warning will appear if payment rate entered is greater than (10,000%) above National rate. Payment rate is defined as the rate per test.

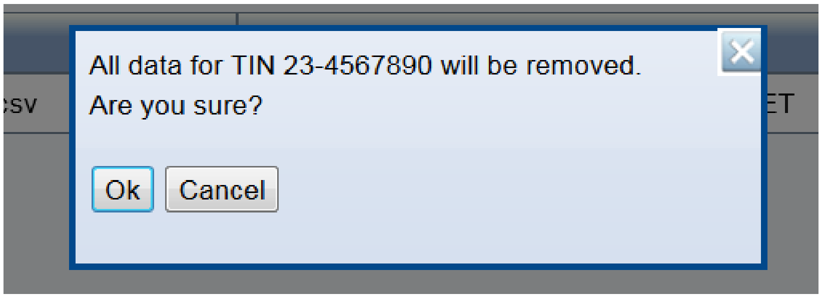
c. Volume: numeric
not a negative value
can be zero
no decimal places
up to 6 digits

d. NPI: numeric
10 digits fixed
no decimal places
cannot have 5 consecutive same digits
must pass Luhn check digit formula

3. Click on "Data Reporting" from the menu on the left side of the screen, click on "Upload Applicable Information," and re-upload your file.
4. To remove a file, click on the **Remove** button next to the applicable file.
5. To remove all the files, click on the **Remove All Files** button.

   A pop-up box displays asking if you are sure you want to remove all the files for the selected TIN as shown in Figure 5-15.

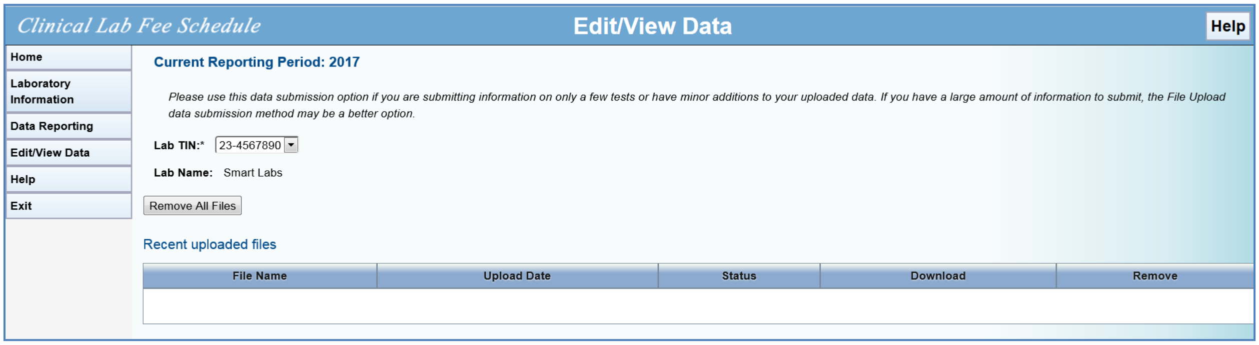
Figure 5-15: TIN Removal Pop-Up


All data for TIN 23-4567890 will be removed.
Are you sure?

6. Click on the **Ok** button.

   All the files are removed for the selected TIN as shown in Figure 5-16.

Figure 5-16: Edit/View Page with File(s) Removed



Current Reporting Period: 2017

Please use this data submission option if you are submitting information on only a few tests or have minor additions to your uploaded data. If you have a large amount of information to submit, the File Upload data submission method may be a better option.

Lab TIN:* 23-4567890

Lab Name: Smart Labs

Recent uploaded files

File Name	Upload Date	Status	Download	Remove

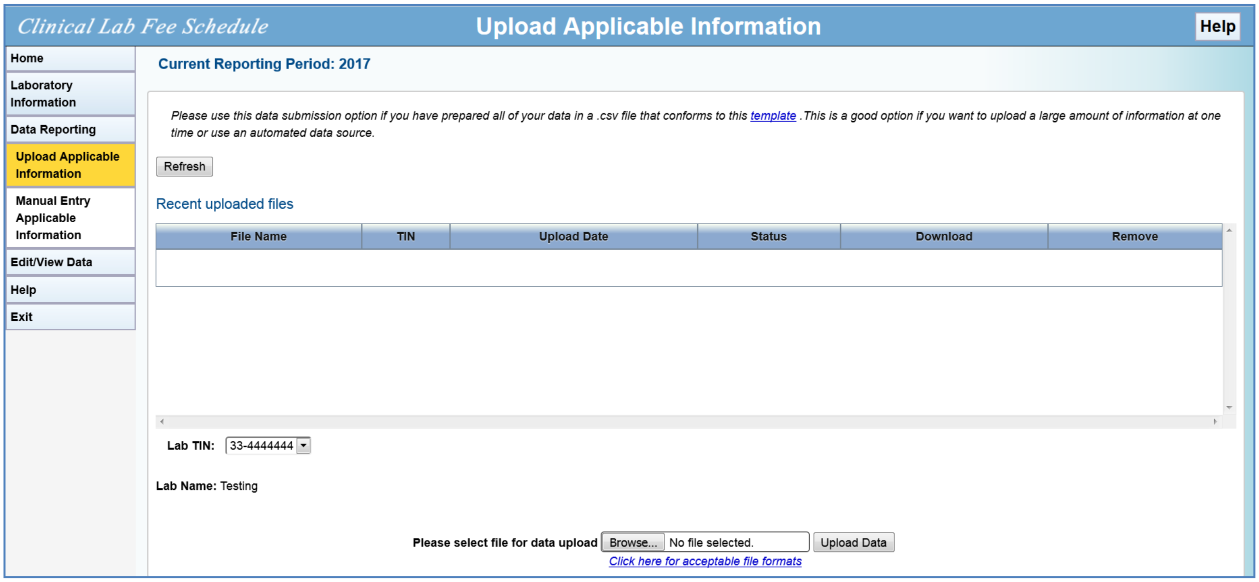
5.3 Upload Applicable Information – CLFS Submitter Very Large Volume (VLV) Role

The CLFS application provides applicable laboratories the ability to report applicable information to CMS using a file transfer process. If the file being uploaded is greater than 29,360,128 bytes, it is considered a Very Large Volume (VLV) file. Once a VLV file is uploaded your role will be modified to a VLV Submitter. Perform the following steps to enter data using the upload process:

1. Log in as CLFS Submitter and click on **Data Reporting** and then click on **Upload Applicable Information**.

   The "Upload Applicable Information" page displays as shown in Figure 5-17.

Figure 5-17: Upload Applicable Information


Clinical Lab Fee Schedule
Upload Applicable Information
Help
Home
Laboratory Information
Data Reporting
Upload Applicable Information
Manual Entry Applicable Information
Edit/View Data
Help
Exit
Refresh
Browse...
Upload Data

Current Reporting Period: 2017

Please use this data submission option if you have prepared all of your data in a .csv file that conforms to this template . This is a good option if you want to upload a large amount of information at one time or use an automated data source.

Recent uploaded files

File Name	TIN	Upload Date	Status	Download	Remove

Lab TIN: 33-4444444

Lab Name: Testing

Please select file for data upload No file selected.

Click here for acceptable file formats

At the top center of the page is a link to the data reporting template that could be used to enter data in .csv format. Previous upload submissions will be displayed at the upper portion of the page.

Note: Template Requirements

- You may change the filename
- Do not add additional columns to the template
- Do not add, remove, or otherwise change columns or column headings within the template
- Do not submit blank rows between data entries
- You must submit all data in contiguous rows

- Enter the HCPCS Code, Payment Rate, Volume, and NPI. The basic edits for the data items are:

  a. HCPCS Code: alphanumeric or all numeric
  5 characters

  b. Payment Rate: numeric
  not a negative value
  999.99 format

  Checked against current CLFS rate; a warning will appear if payment rate entered is greater than (10,000%) above National rate. Payment rate is defined as the rate per test.

  c. Volume: numeric
  not a negative value
  can be zero
  no decimal places
  up to 6 digits

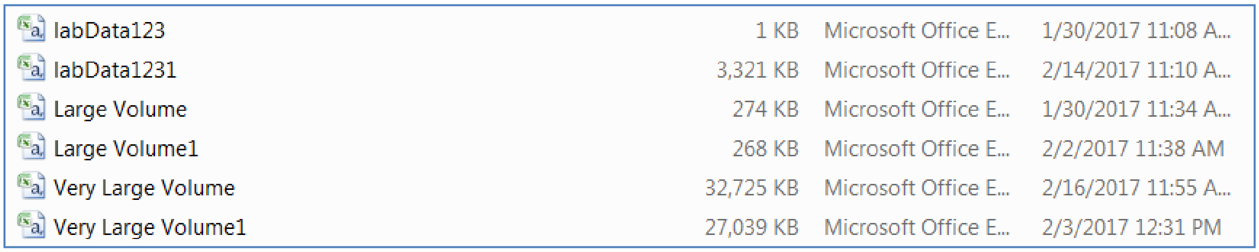
  d. NPI: numeric
  10 digits fixed
  no decimal places
  cannot have 5 consecutive same digits
  must pass Luhn check digit formula

The **Refresh** button is used when a submission is taking an extended period to process. By clicking on the **Refresh** button, the Submitter can see if the file upload is still processing or completed

2. To upload the data, click on the **Browse…** button.

   The file directory window displays as shown in Figure 5-18.

Figure 5-18: File Director Window - VLV

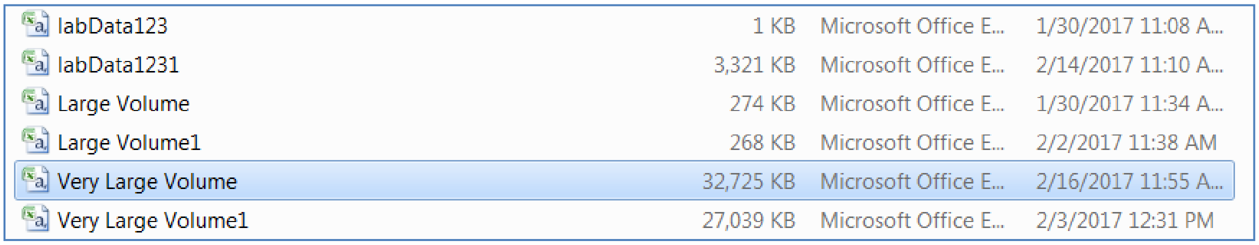


labData123	1 KB	Microsoft Office E...	1/30/2017 11:08 A...
labData1231	3,321 KB	Microsoft Office E...	2/14/2017 11:10 A...
Large Volume	274 KB	Microsoft Office E...	1/30/2017 11:34 A...
Large Volume1	268 KB	Microsoft Office E...	2/2/2017 11:38 AM
Very Large Volume	32,725 KB	Microsoft Office E...	2/16/2017 11:55 A...
Very Large Volume1	27,039 KB	Microsoft Office E...	2/3/2017 12:31 PM

3. Select the directory path and filename to upload.

   The filename appears in the "File name" window, as shown in Figure 5-19.

Figure 5-19: File Director Window – VLV File Selected

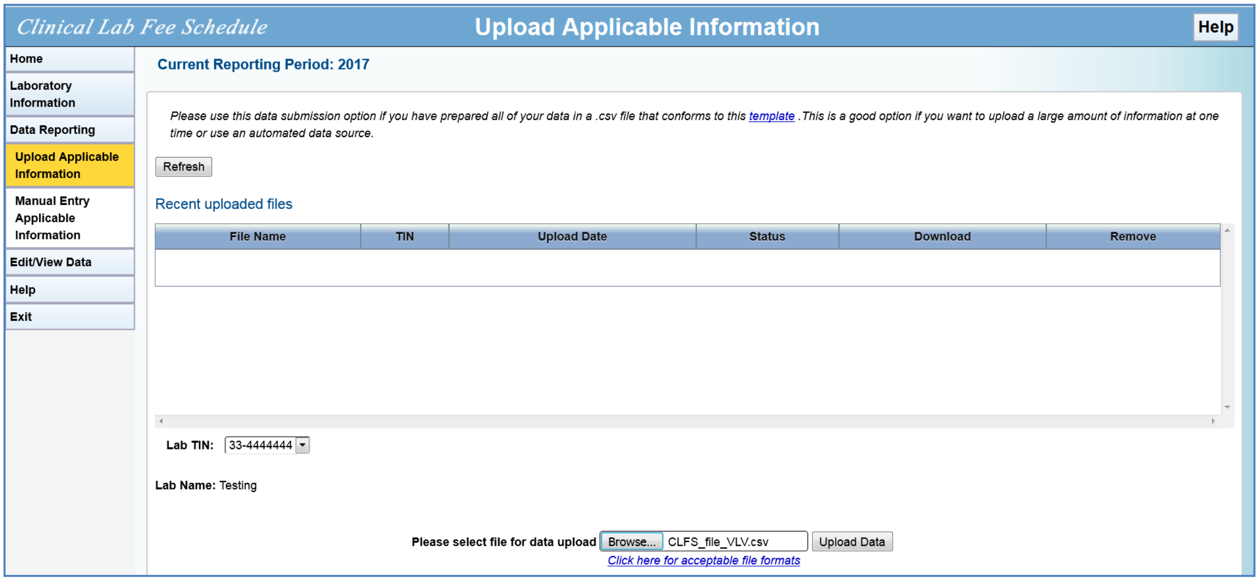


labData123	1 KB	Microsoft Office E...	1/30/2017 11:08 A...
labData1231	3,321 KB	Microsoft Office E...	2/14/2017 11:10 A...
Large Volume	274 KB	Microsoft Office E...	1/30/2017 11:34 A...
Large Volume1	268 KB	Microsoft Office E...	2/2/2017 11:38 AM
Very Large Volume	32,725 KB	Microsoft Office E...	2/16/2017 11:55 A...
Very Large Volume1	27,039 KB	Microsoft Office E...	2/3/2017 12:31 PM

4. Click on the **Open** button.

   The filename appears in the “Browse” window, as shown in Figure 5-20.

Figure 5-20: File Director Window – VLV File Displayed



Clinical Lab Fee Schedule
Upload Applicable Information
Help
Home
Laboratory Information
Data Reporting
Upload Applicable Information
Manual Entry Applicable Information
Edit/View Data
Help
Exit

Current Reporting Period: 2017

Please use this data submission option if you have prepared all of your data in a .csv file that conforms to this template . This is a good option if you want to upload a large amount of information at one time or use an automated data source.

Recent uploaded files

File Name	TIN	Upload Date	Status	Download	Remove

Lab TIN: 33-4444444

Lab Name: Testing

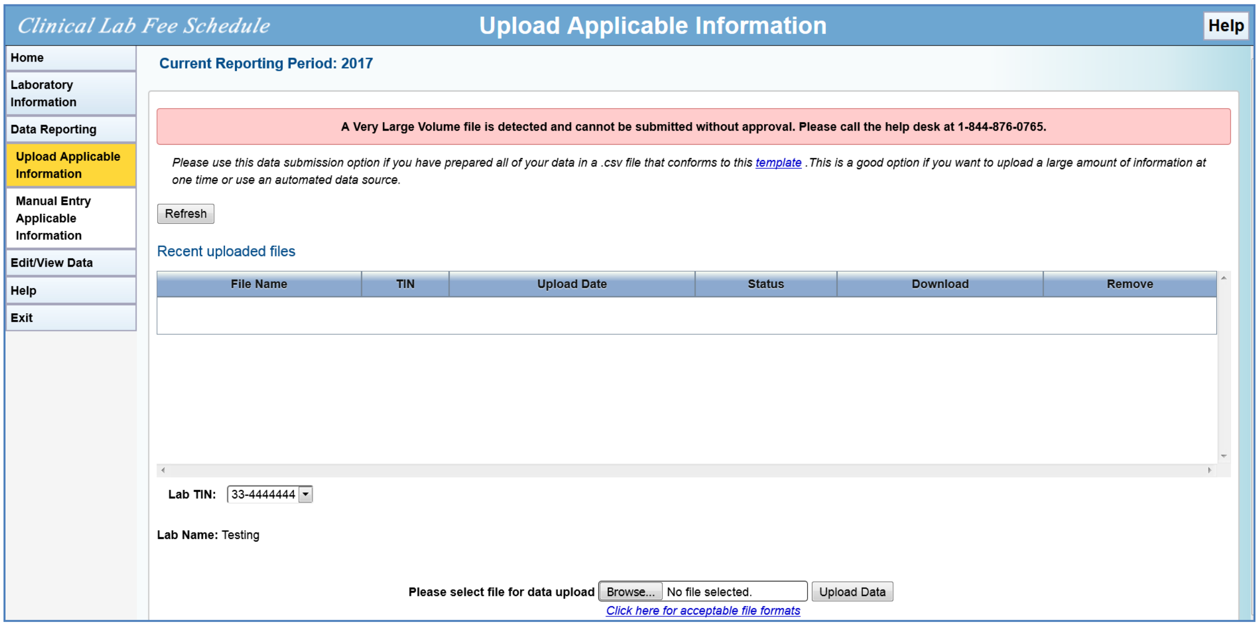
Please select file for data upload Browse... CLFS_file_VLV.csv Upload Data

Click here for acceptable file formats

5. Click on the **Upload Data** button.

   Note: if the role of the Submitter is set to “Normal” or “LV,” a banner displays to have the Submitter contact the Help Desk to have their role changed to “VLV” as shown in Figure 5-21. Once the role has been changed, repeat Steps 1 through 5.

Figure 5-21: File Director Window – VLV File Detected – Contact Help Desk


Clinical Lab Fee Schedule
Upload Applicable Information
Help
Home
Laboratory Information
Data Reporting
Upload Applicable Information
Manual Entry Applicable Information
Edit/View Data
Help
Exit
Refresh
Browse...
Upload Data

Current Reporting Period: 2017

A Very Large Volume file is detected and cannot be submitted without approval. Please call the help desk at 1-844-876-0765.

Please use this data submission option if you have prepared all of your data in a .csv file that conforms to this template .This is a good option if you want to upload a large amount of information at one time or use an automated data source.

Recent uploaded files

File Name	TIN	Upload Date	Status	Download	Remove

Lab TIN: 33-4444444

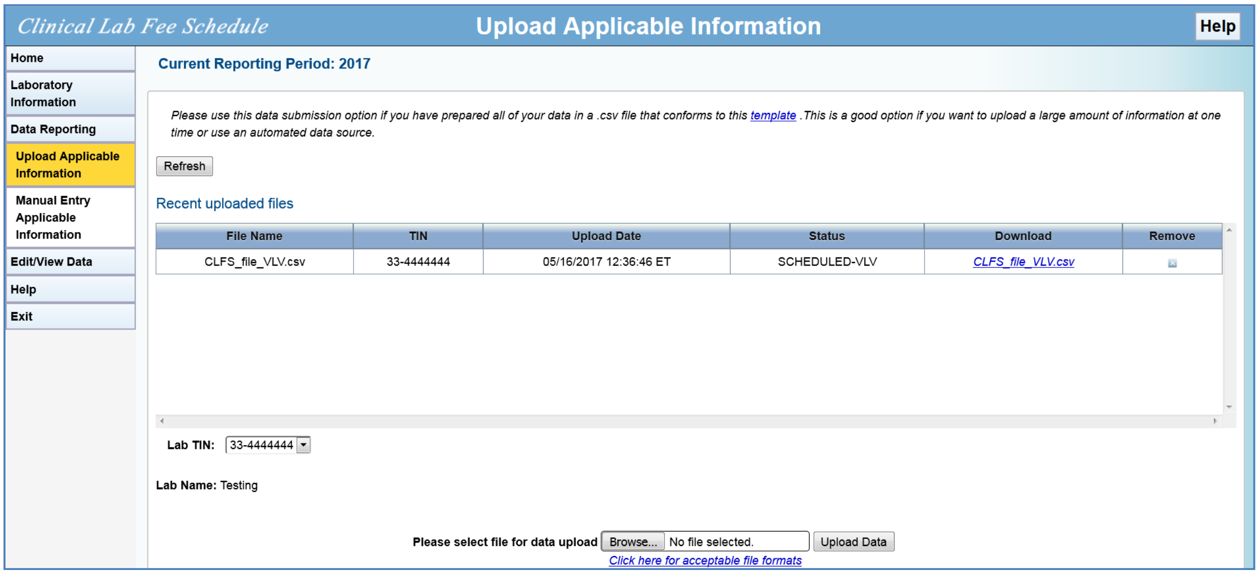
Lab Name: Testing

Please select file for data upload No file selected.

Click here for acceptable file formats

The file to upload displays with the Status as “SCHEDULED-VLV,” as shown in Figure 5-22.

Figure 5-22: File Director Window – VLV File Scheduled


Clinical Lab Fee Schedule
Upload Applicable Information
Help
Home
Laboratory Information
Data Reporting
Upload Applicable Information
Manual Entry Applicable Information
Edit/View Data
Help
Exit
Refresh
Browse...
Upload Data

Current Reporting Period: 2017

Please use this data submission option if you have prepared all of your data in a .csv file that conforms to this template . This is a good option if you want to upload a large amount of information at one time or use an automated data source.

Recent uploaded files

File Name	TIN	Upload Date	Status	Download	Remove
CLFS_file_VLV.csv	33-4444444	05/16/2017 12:36:46 ET	SCHEDULED-VLV	CLFS_file_VLV.csv	

Lab TIN: 33-4444444

Lab Name: Testing

Please select file for data upload No file selected.

Click here for acceptable file formats

Note: The Submitter will need to wait until the CMS Admin processes the VLV file and notifies them that the processing has been completed.

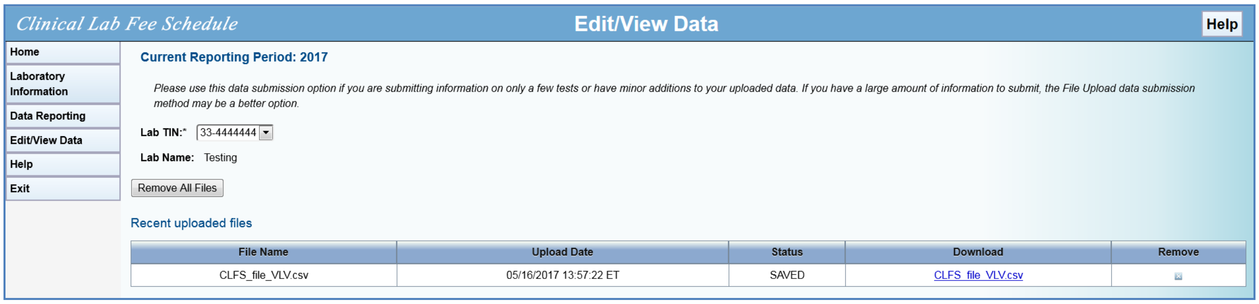
5.3.1 Edit/View Data – CLFS Submitter Very Large Volume Role

The CLFS application provides applicable laboratories the ability to edit information to CMS. Perform the following steps to edit data. Once the CMS Administrator has sent a notification that the Very Large Volume file that was submitted has been processed perform the following steps.

1. Log in as CLFS Submitter and click on Edit/View Data.

   The "Edit/View Data" window displays, as shown in Figure 5-23.

Figure 5-23: Very Large Volume Edit/View Page



Current Reporting Period: 2017

Please use this data submission option if you are submitting information on only a few tests or have minor additions to your uploaded data. If you have a large amount of information to submit, the File Upload data submission method may be a better option.

Lab TIN:* 33-4444444

Lab Name: Testing

Recent uploaded files

File Name	Upload Date	Status	Download	Remove
CLFS_file_VLV.csv	05/16/2017 13:57:22 ET	SAVED	CLFS_file_VLV.csv	

2. To edit data, click the file link in the "Download" section, and edit change the information in the .csv file. The basic edits for the data items are:

a. HCPCS Code:	alphanumeric or all numeric 5 characters
b. Payment Rate:	numeric not a negative value 999.99 format

Checked against current CLFS rate; a warning will appear if payment rate entered is greater than (10,000%) above National rate. Payment rate is defined as the rate per test.

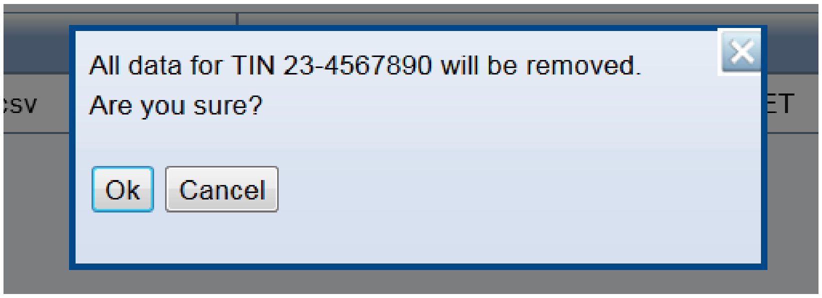
c. Volume:
numeric
not a negative value
can be zero
no decimal places
up to 6 digits

d. NPI:
numeric
10 digits fixed
no decimal places
cannot have 5 consecutive same digits
must pass Luhn check digit formula

3. Click on "Data Reporting" from the menu on the left side of the screen, click on "Upload Applicable Information," and re-upload your file.
4. To remove a file, click on the **Remove** button next to the applicable file.
5. To remove all the files, click on the **Remove All Files** button.

   A pop-up box displays asking if you are sure you want to remove all the files for the selected TIN as shown in Figure 5-24.

Figure 5-24: TIN Removal Pop-Up

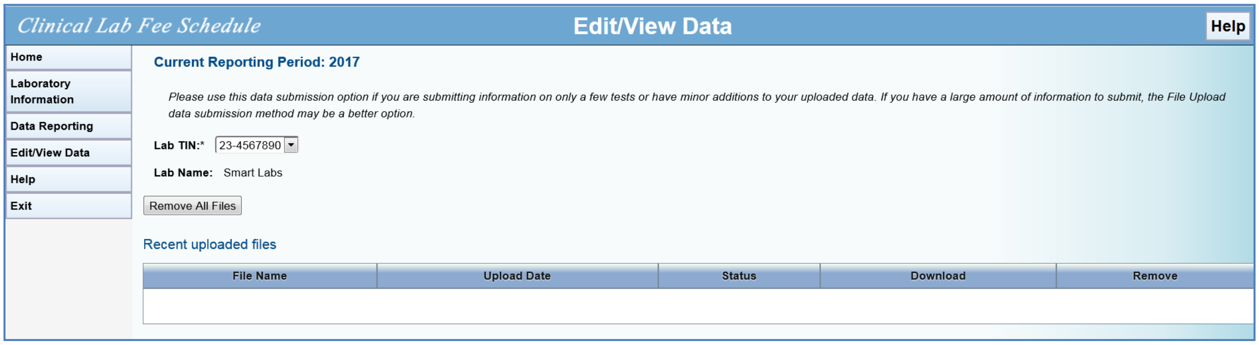


All data for TIN 23-4567890 will be removed.
Are you sure?

6. Click on the **Ok** button.

   All the files are removed for the selected TIN as shown in Figure 5-25.

Figure 5-25: Edit/View Page with File(s) Removed



Current Reporting Period: 2017

Please use this data submission option if you are submitting information on only a few tests or have minor additions to your uploaded data. If you have a large amount of information to submit, the File Upload data submission method may be a better option.

Lab TIN:* 23-4567890

Lab Name: Smart Labs

Recent uploaded files

File Name	Upload Date	Status	Download	Remove

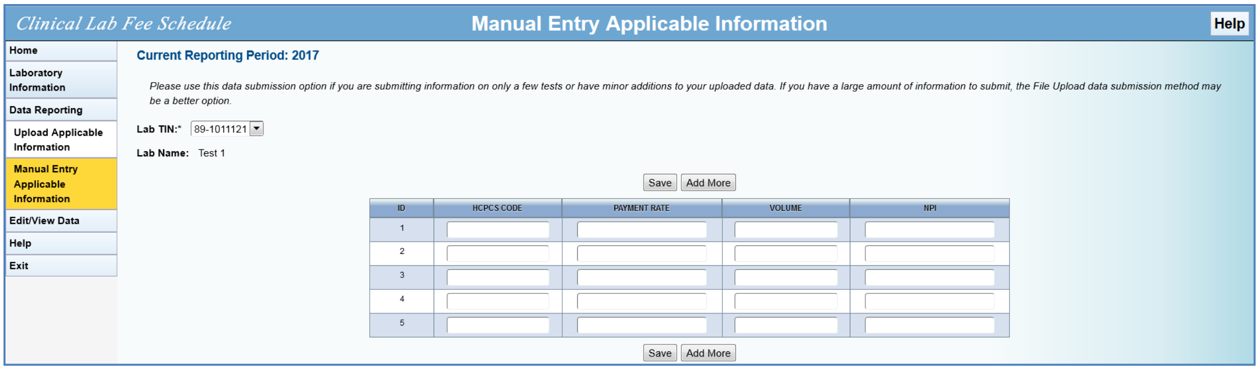
5.4 Manual Entry – CLFS Submitter

The CLFS application provides applicable laboratories the ability to report applicable information to CMS using manual key-in entry of data. Perform the following steps to enter data using the manual data entry process.

1. Log in as CLFS Submitter, click on **Data Reporting** from the left side of the screen, and then click on **Manual Entry Applicable Information**.

   The “Manual Entry Applicable Information” page displays as shown in Figure 5-26.

   Figure 5-26: Manual Entry Applicable Information Page


Clinical Lab Fee Schedule
Manual Entry Applicable Information
Help
Home
Laboratory Information
Data Reporting
Upload Applicable Information
Manual Entry Applicable Information
Edit/View Data
Help
Exit
Save
Add More

Current Reporting Period: 2017

Please use this data submission option if you are submitting information on only a few tests or have minor additions to your uploaded data. If you have a large amount of information to submit, the File Upload data submission method may be a better option.

Lab TIN:* 89-1011121

Lab Name: Test 1

ID	HCPCS CODE	PAYMENT RATE	VOLUME	NPI
1				
2				
3				
4				
5				

   Note: If multiple TINs are registered, select a TIN from the “Lab TIN:” dropdown list.

2. Enter the HCPCS Code, Payment Rate, Volume, and NPI.

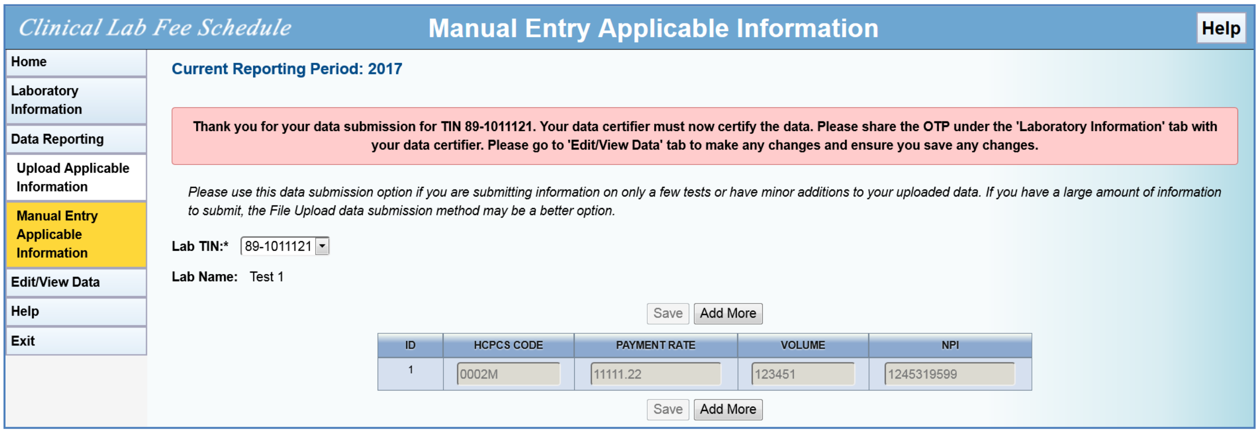
   The basic edits for the data items are:

   a. HCPCS Code: alphanumeric or all numeric
      5 characters
   b. Payment Rate: numeric
      not a negative value
      999.99 format
      Checked against current CLFS rate; a warning will appear if payment rate entered is greater than (10,000%) above National rate. Payment rate is defined as the rate per test.
   c. Volume: numeric
      not a negative value
      can be zero
      no decimal places
   d. NPI: numeric
      10 digits fixed
      no decimal places
      cannot have 5 consecutive same digits
      must pass Luhn check digit formula

3. Click on the **Save** button.

   The screen displays the confirmation that the data have been successfully saved with further instructions, either to have the CLFS Certifier certify the data or to go to the “Edit/View Data” screen to change data, as shown in Figure 5-27. If there are validation errors, the application will display an error message at the field in error.

Figure 5-27: Manual Entry Applicable Information – Data Submission Confirmation Page


Clinical Lab Fee Schedule
Manual Entry Applicable Information
Help
Home
Laboratory Information
Data Reporting
Upload Applicable Information
Manual Entry Applicable Information
Edit/View Data
Help
Exit
Save
Add More

Current Reporting Period: 2017

Thank you for your data submission for TIN 89-1011121. Your data certifier must now certify the data. Please share the OTP under the 'Laboratory Information' tab with your data certifier. Please go to 'Edit/View Data' tab to make any changes and ensure you save any changes.

Please use this data submission option if you are submitting information on only a few tests or have minor additions to your uploaded data. If you have a large amount of information to submit, the File Upload data submission method may be a better option.

Lab TIN:* 89-1011121

Lab Name: Test 1

ID	HCPCS CODE	PAYMENT RATE	VOLUME	NPI
1	0002M	11111.22	123451	1245319599

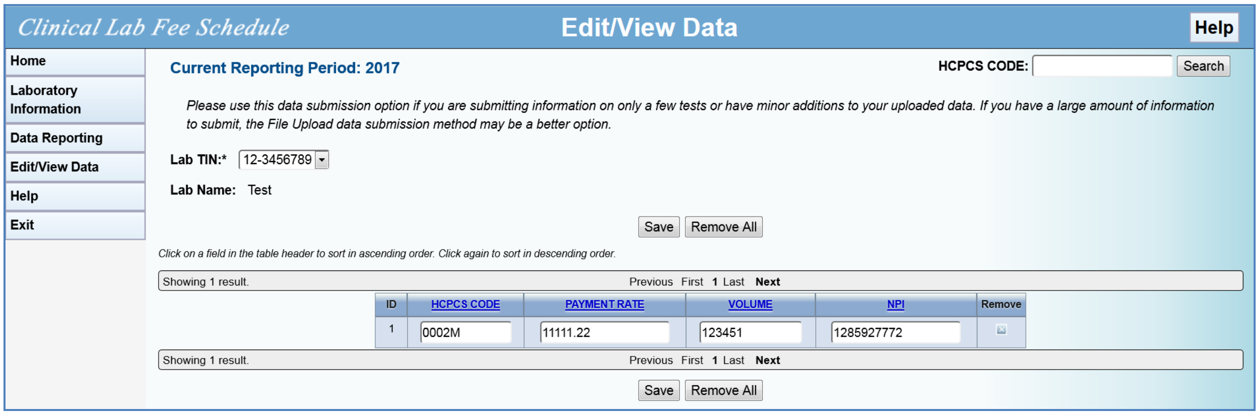
5.4.1 Edit/View Data

The CLFS application provides applicable laboratories the ability to edit information to CMS. Perform the following steps to edit data.

1. Log in as CLFS Submitter and click on **Edit/View Data**.

   The “Edit/View Data” window displays as shown in Figure 5-28.

Figure 5-28: Manual Entry - Edit/View Data Page



Current Reporting Period: 2017

HCPCS CODE:

Please use this data submission option if you are submitting information on only a few tests or have minor additions to your uploaded data. If you have a large amount of information to submit, the File Upload data submission method may be a better option.

Lab TIN:* 12-3456789

Lab Name: Test

Click on a field in the table header to sort in ascending order. Click again to sort in descending order.

Showing 1 result.

ID	HCPCS CODE	PAYMENT RATE	VOLUME	NPI	Remove
1	0002M	11111.22	123451	1285927772	□

Showing 1 result.

2. The data can be sorted in ascending or descending order clicking on any of the headers. Click on the header once for ascending order, click again for descending order.

   The application will show how many records there are.

3. To edit data, click in any of the fields and change the information. The basic edits for the data items are:

   a. HCPCS Code: alphanumeric or all numeric
      5 characters
   b. Payment Rate: numeric
      not a negative value
      999.99 format

Checked against current CLFS rate; a warning will appear if payment rate entered is greater than (10,000%) above National rate. Payment rate is defined as the rate per test.

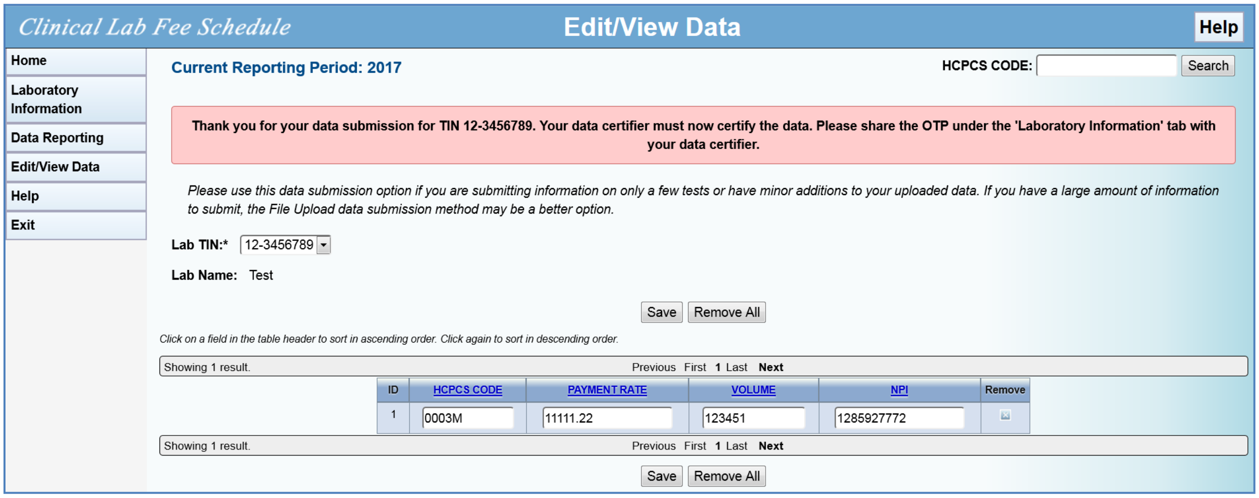
c. Volume: numeric
not a negative value
can be zero
no decimal places

d. NPI: numeric
10 digits fixed
no decimal places
cannot have 5 consecutive same digits
must pass Luhn check digit formula

The application displays the change made in the field and a message displays stating that the data needs to be certified.

If there are any data entries that need to be removed, the user can click on the **X** box under the "Remove" column. If all the data entries need to be removed, the user can click on the **Remove All** button and the data for the selected TIN will be removed, as shown in Figure 5-29.

Figure 5-29: Manual Entry - Edit Data Confirmation



Current Reporting Period: 2017

HCPCS CODE:

Thank you for your data submission for TIN 12-3456789. Your data certifier must now certify the data. Please share the OTP under the 'Laboratory Information' tab with your data certifier.

Please use this data submission option if you are submitting information on only a few tests or have minor additions to your uploaded data. If you have a large amount of information to submit, the File Upload data submission method may be a better option.

Lab TIN:* 12-3456789

Lab Name: Test

Click on a field in the table header to sort in ascending order. Click again to sort in descending order.

Showing 1 result.

ID	HCPCS CODE	PAYMENT RATE	VOLUME	NPI	Remove
1	0003M	11111.22	123451	1285927772	☒

Showing 1 result.

6. CLFS Certifier Registration

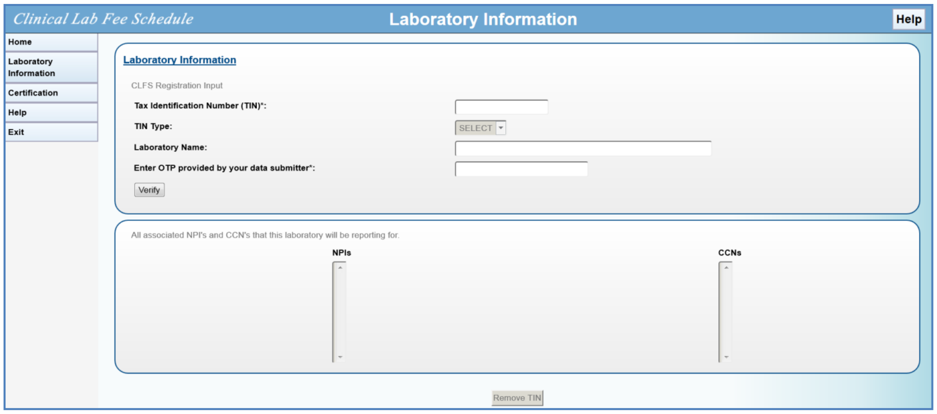
6.1 Laboratory Information/Verify One Time Password (OTP) – CLFS Certifier

To verify the relationship between the CLFS Submitter and the Certifier, a CLFS Certifier must enter the applicable information and the OTP sent to them by the CLFS Submitter.

1. CLFS Certifier logs into the application.

   The "Laboratory Information" screen displays as shown in Figure 6-1.

Figure 6-1: Certifier - Laboratory Information Window



CLFS Registration Input

Tax Identification Number (TIN)*:

TIN Type:

Laboratory Name:

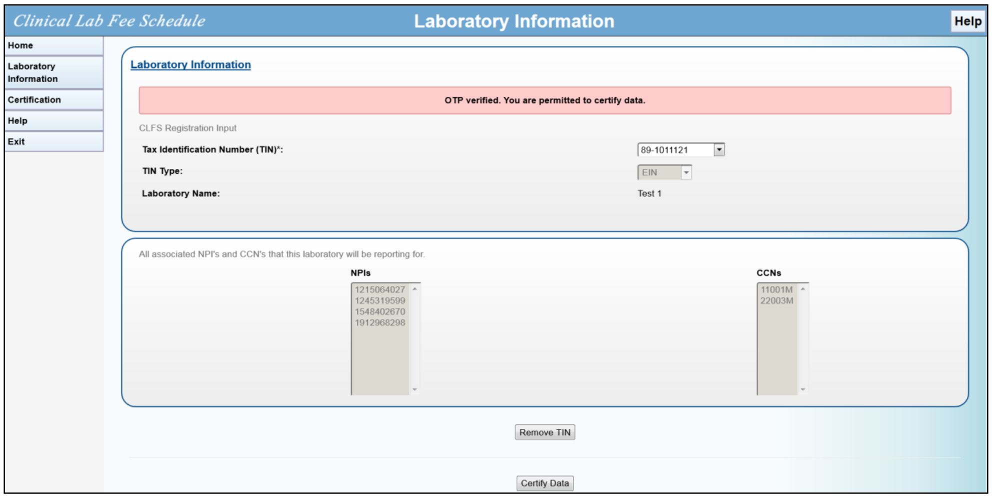
Enter OTP provided by your data submitter*:

All associated NPI's and CCN's that this laboratory will be reporting for.

2. Enter the following fields:
   a. TIN(s) provided by the CLFS Submitter
   b. Lab Name (Optional)
   c. The OTP provided by the CLFS Submitter for all TINS.
3. Click on the **Verify** button to verify the OTP.

   A verification message that the OTP has been certified displays as shown in Figure 6-2.

Figure 6-2: Laboratory Information – OTP Verified Window



OTP verified. You are permitted to certify data.

CLFS Registration Input

Tax Identification Number (TIN)*: 89-1011121

TIN Type: EIN

Laboratory Name: Test 1

All associated NPI's and CCN's that this laboratory will be reporting for.

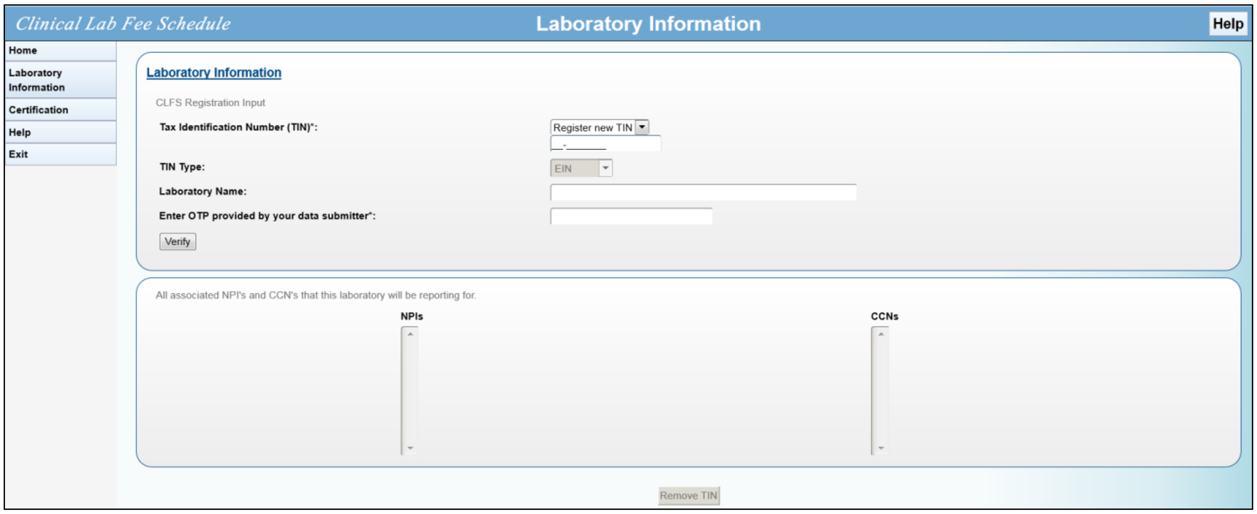
NPIs: 1215064027, 1245319599, 1548402670, 1912968298

CCNs: 11001M, 22003M

Note: If the OTP has expired, have the CLFS Submitter generate another OTP and try again.

4. To add another TIN to certify, select "Register new TIN" from the TIN drop-down menu as shown in Figure 6-3.

Figure 6-3: Laboratory Information – Register New TIN



Tax Identification Number (TIN)*: Register new TIN

TIN Type: EIN

Laboratory Name:

Enter OTP provided by your data submitter*:

Verify
All associated NPI's and CCN's that this laboratory will be reporting for.
NPIs
CCNs
Remove TIN

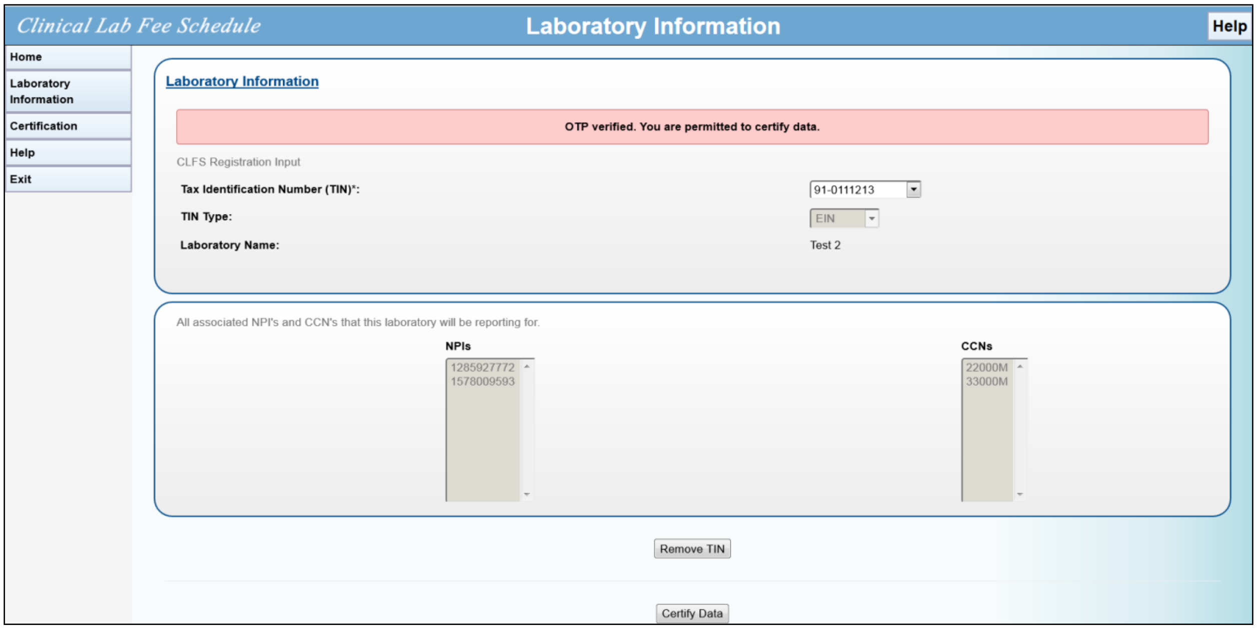
5. Enter the following fields:

   a. TIN
   b. The OTP provided by the CLFS Submitter

6. Click on the **Verify** button to verify the OTP.

   A verification message that the OTP has been verified displays, as shown in Figure 6-4.

Figure 6-4: Laboratory Information – OTP Verified Window



OTP verified. You are permitted to certify data.

Tax Identification Number (TIN)*: 91-0111213

TIN Type: EIN

Laboratory Name: Test 2

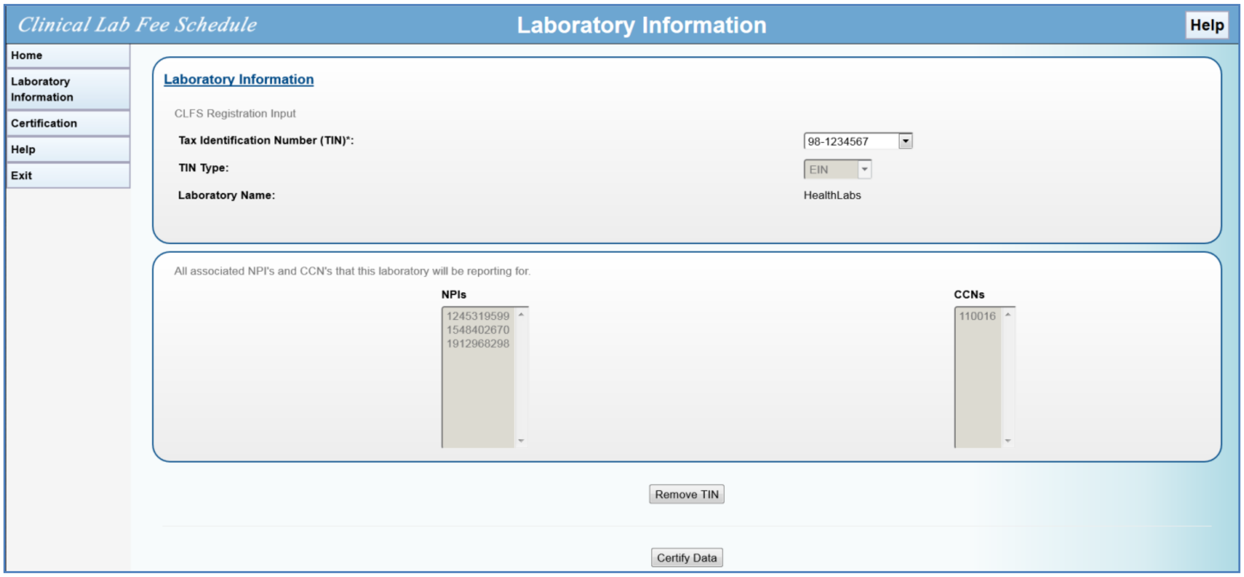
All associated NPI's and CCN's that this laboratory will be reporting for.

NPIs: 1285927772, 1578009593

CCNs: 22000M, 33000M

7. To remove a TIN, select a TIN from the TIN drop-down menu, as shown in Figure 6-5.

Figure 6-5: Laboratory Information – TIN to be Removed



CLFS Registration Input

Tax Identification Number (TIN)*: 98-1234567

TIN Type: EIN

Laboratory Name: HealthLabs

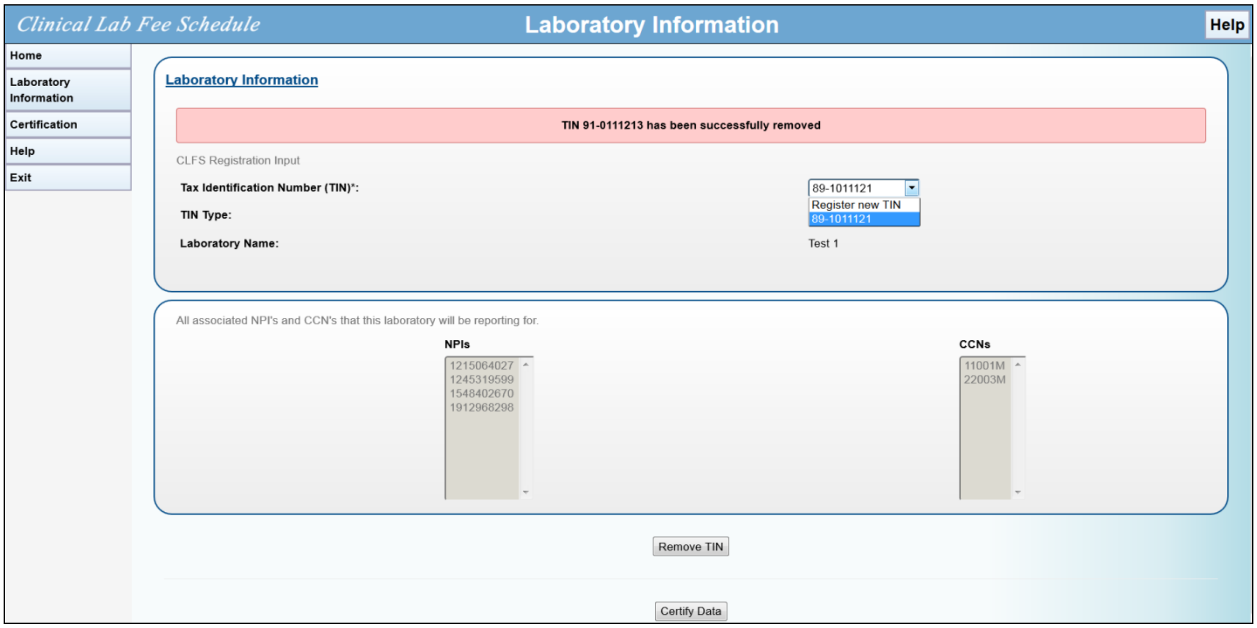
All associated NPI's and CCN's that this laboratory will be reporting for.

NPIs	CCNs
1245319599 1548402670 1912968298	110016

8. Click on the **Remove TIN** button.

   A verification message displays stating that the selected TIN has been successfully removed, and the dropdown list no longer contains the removed TIN, as shown in Figure 6-6.

Figure 6-6: Laboratory Information – Selected TIN Removed Message



TIN 91-0111213 has been successfully removed

CLFS Registration Input

Tax Identification Number (TIN)*: 89-1011121

TIN Type:

Laboratory Name: Test 1

All associated NPI's and CCN's that this laboratory will be reporting for.

NPIs	CCNs
1215064027 1245319599 1548402670 1912968298	11001M 22003M

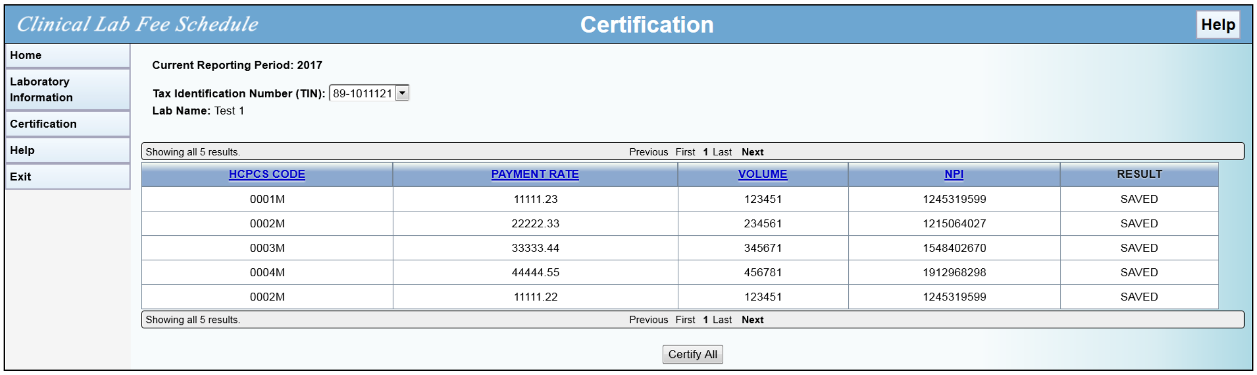
7. Certification

Data certification is a process where an applicable laboratory representative (CLFS Certifier) certifies the accuracy of the data. The CLFS Certifier must certify all data items pending certification. The CLFS certifier cannot make any edits to the data. If the CLFS certifier identifies a need to edit data, this must be completed by the CLFS submitter.

1. CLFS Certifier logs and clicks on “Certification” from the left side of the screen.

   The “Certification” window displays as shown in Figure 7-1.

Figure 7-1: Certification Window



Current Reporting Period: 2017

Tax Identification Number (TIN): 89-1011121

Lab Name: Test 1

Showing all 5 results.

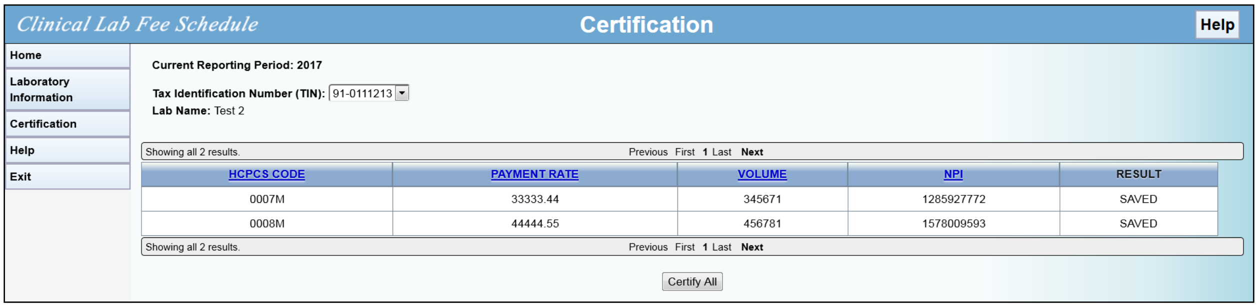
HCPCS CODE	PAYMENT RATE	VOLUME	NPI	RESULT
0001M	11111.23	123451	1245319599	SAVED
0002M	22222.33	234561	1215064027	SAVED
0003M	33333.44	345671	1548402670	SAVED
0004M	44444.55	456781	1912968298	SAVED
0002M	11111.22	123451	1245319599	SAVED

Showing all 5 results.

2. Select a TIN from the drop-down box.

   The data for the selected TIN display as shown in Figure 7-2.

Figure 7-2: Selected TIN Data to be Certified



Current Reporting Period: 2017

Tax Identification Number (TIN): 91-0111213

Lab Name: Test 2

Showing all 2 results.

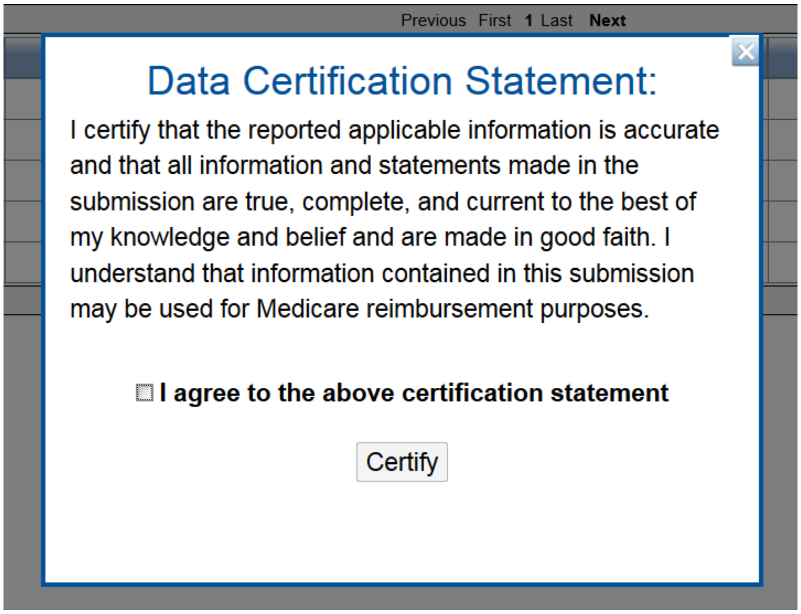
HCPCS CODE	PAYMENT RATE	VOLUME	NPI	RESULT
0007M	33333.44	345671	1285927772	SAVED
0008M	44444.55	456781	1578009593	SAVED

Showing all 2 results.

3. Click on the **Certify All** button.

   A “Data Certification Statement” pop-up window displays as shown in Figure 7-3.

Figure 7-3: Data Certification Statement



Data Certification Statement:

I certify that the reported applicable information is accurate and that all information and statements made in the submission are true, complete, and current to the best of my knowledge and belief and are made in good faith. I understand that information contained in this submission may be used for Medicare reimbursement purposes.

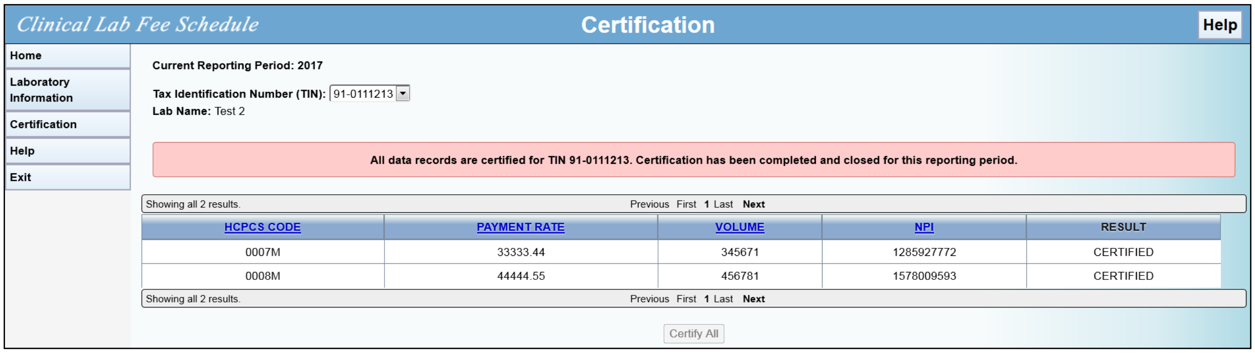
☐ **I agree to the above certification statement**

4. Review the statement, click in the box next to “I agree to the above certification statement,” and then click on the **Certify** button.

   Note: The application will display a message “All data records are certified. Certification has been completed and closed for this reporting period.”

   All the “Results” for the data changes are changed from being “SAVED” to “CERTIFIED” as shown in Figure 7-4.

Figure 7-4: Certification - Data Certified Window



Current Reporting Period: 2017

Tax Identification Number (TIN): 91-0111213

Lab Name: Test 2

All data records are certified for TIN 91-0111213. Certification has been completed and closed for this reporting period.

Showing all 2 results. Previous First 1 Last Next

HCPCS CODE	PAYMENT RATE	VOLUME	NPI	RESULT
0007M	33333.44	345671	1285927772	CERTIFIED
0008M	44444.55	456781	1578009593	CERTIFIED

Showing all 2 results. Previous First 1 Last Next

Warning: Once the CLFS Certifier has certified the data for the current period, data submission is closed, and no more data can be entered for that TIN. Be sure that all applicable information is entered, accurate, and complete before certifying the data. If corrections need to be made post certification, please contact the CLFS helpdesk:

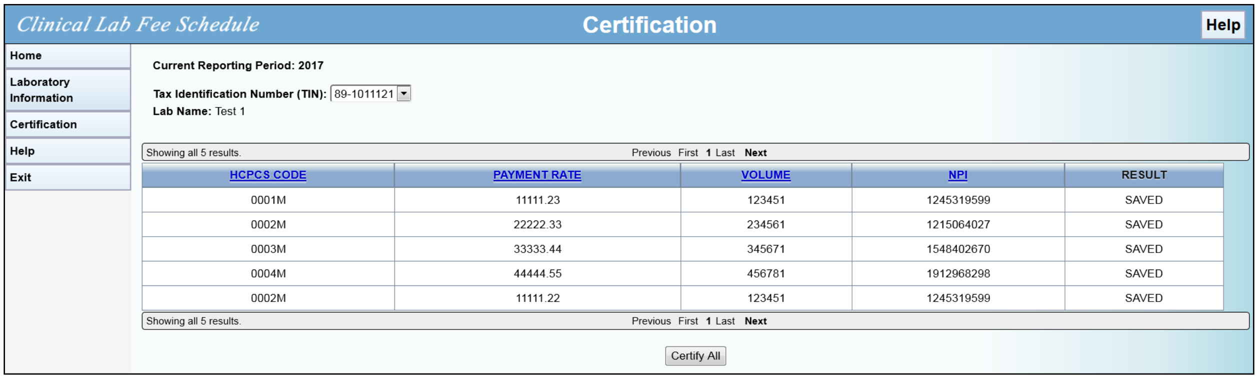
Application Help Desk

- E-mail: CLFSHelpDesk@dcca.com
- Phone: 844-876-0765
  - 9AM-6PM Eastern, Non-Peak
  - 9AM-9PM Eastern, Peak (i.e., January-March 2017)

5. To certify data for another TIN, select another TIN from the TIN dropdown menu.

   The data for the selected TIN display as shown in Figure 7-5.

Figure 7-5: Certification – Certify Another TIN



Current Reporting Period: 2017

Tax Identification Number (TIN): 89-1011121

Lab Name: Test 1

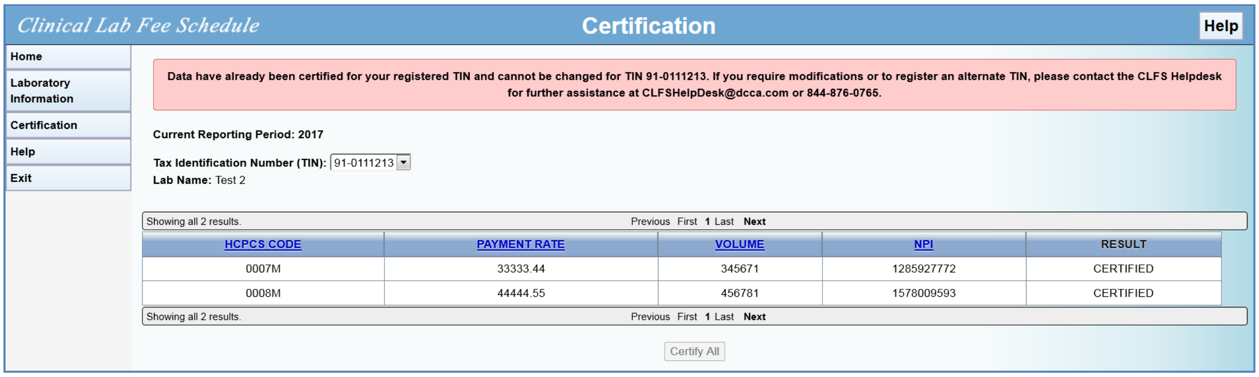
Showing all 5 results.

HCPCS CODE	PAYMENT RATE	VOLUME	NPI	RESULT
0001M	11111.23	123451	1245319599	SAVED
0002M	22222.33	234561	1215064027	SAVED
0003M	33333.44	345671	1548402670	SAVED
0004M	44444.55	456781	1912968298	SAVED
0002M	11111.22	123451	1245319599	SAVED

Showing all 5 results.

Note: if you select a TIN where data have already been certified, you will receive a message stating that the data have already been certified for the selected TIN, as shown in Figure 7-6.

Figure 7-6: Certification – Selected TIN has Already Been Certified Message



Data have already been certified for your registered TIN and cannot be changed for TIN 91-0111213. If you require modifications or to register an alternate TIN, please contact the CLFS Helpdesk for further assistance at CLFSHelpDesk@dcca.com or 844-876-0765.

Current Reporting Period: 2017

Tax Identification Number (TIN): 91-0111213

Lab Name: Test 2

Showing all 2 results.

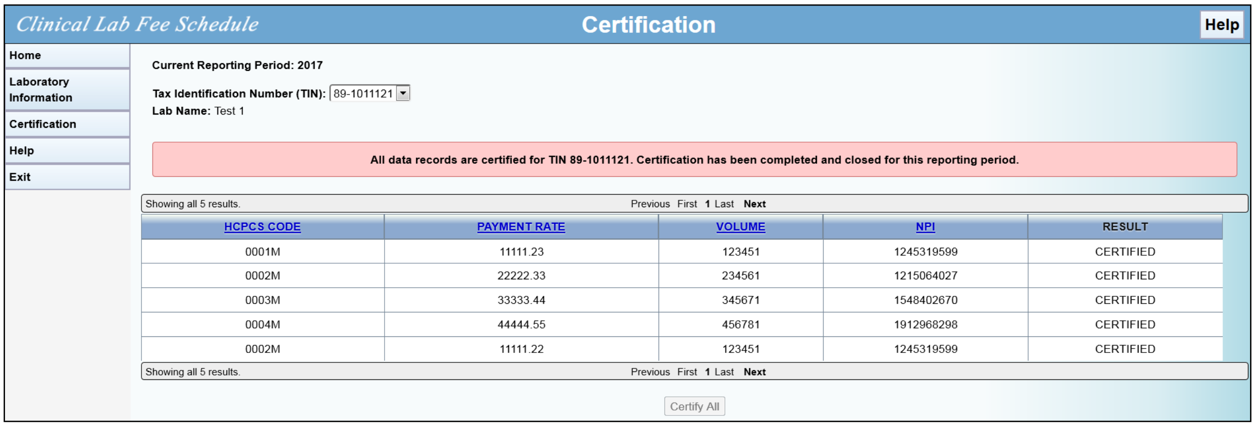
HCPCS CODE	PAYMENT RATE	VOLUME	NPI	RESULT
0007M	33333.44	345671	1285927772	CERTIFIED
0008M	44444.55	456781	1578009593	CERTIFIED

Showing all 2 results.

6. Click on the **Certify All** button and repeat step 4.

   All the “Results” for the data changes are changed from being “SAVED” to “CERTIFIED” as shown in Figure 7-7.

Figure 7-7: Certification - Data Certified Window



Current Reporting Period: 2017

Tax Identification Number (TIN): 89-1011121

Lab Name: Test 1

All data records are certified for TIN 89-1011121. Certification has been completed and closed for this reporting period.

Showing all 5 results.

HCPCS CODE	PAYMENT RATE	VOLUME	NPI	RESULT
0001M	11111.23	123451	1245319599	CERTIFIED
0002M	22222.33	234561	1215064027	CERTIFIED
0003M	33333.44	345671	1548402670	CERTIFIED
0004M	44444.55	456781	1912968298	CERTIFIED
0002M	11111.22	123451	1245319599	CERTIFIED

Showing all 5 results.

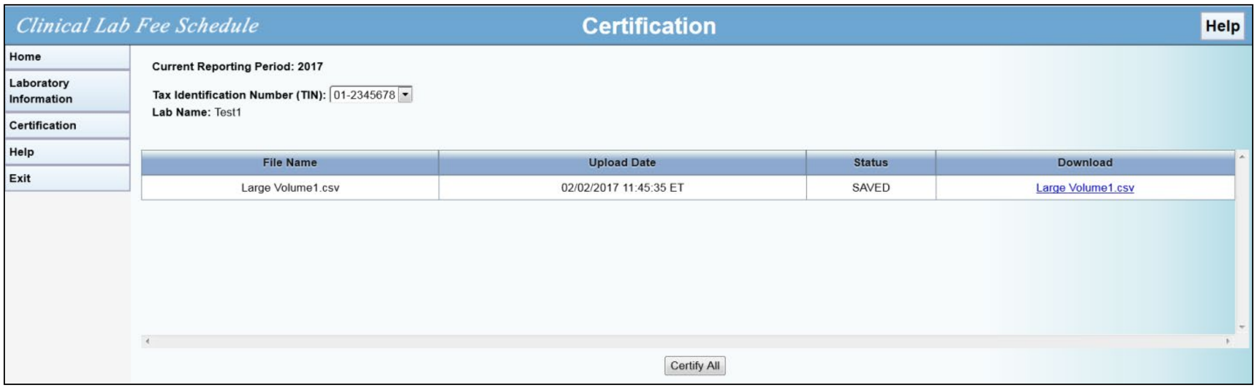
7.1 Certification – Large Volume/Very Large Volume

Data certification is a process where an applicable laboratory representative (CLFS Certifier) certifies the accuracy of the data. The CLFS Certifier must certify all data files pending certification. The CLFS certifier cannot make any edits to the data file. If the CLFS certifier identifies a need to edit the data file, this must be completed by the CLFS submitter.

1. CLFS Certifier logs into the application and clicks on “Certification” from the left side of the screen.

   The “Certification” window displays as shown in Figure 7-8.

Figure 7-8: Certification Window – Large Volume/Very Large Volume



Current Reporting Period: 2017

Tax Identification Number (TIN): 01-2345678

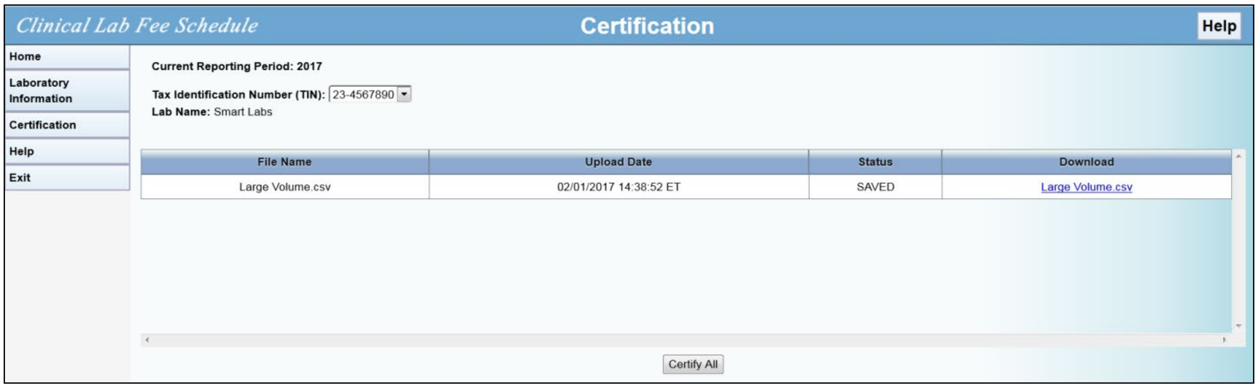
Lab Name: Test1

File Name	Upload Date	Status	Download
Large Volume1.csv	02/02/2017 11:45:35 ET	SAVED	Large Volume1.csv

2. Select a TIN from the drop-down box.

   The file for the selected TIN displays as shown in Figure 7-9.

Figure 7-9: Selected TIN Data to be Certified – Large Volume/Very Large Volume



Current Reporting Period: 2017

Tax Identification Number (TIN): 23-4567890

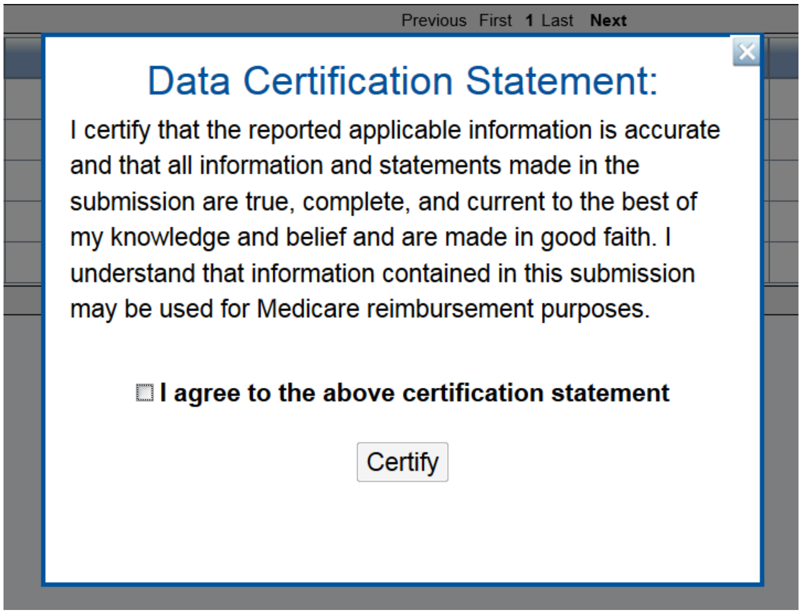
Lab Name: Smart Labs

File Name	Upload Date	Status	Download
Large Volume.csv	02/01/2017 14:38:52 ET	SAVED	Large Volume.csv

3. Click on the **Certify All** button.

   A "Data Certification Statement" pop-up window displays as shown in Figure 7-10.

Figure 7-10: Data Certification Statement



Data Certification Statement:

I certify that the reported applicable information is accurate and that all information and statements made in the submission are true, complete, and current to the best of my knowledge and belief and are made in good faith. I understand that information contained in this submission may be used for Medicare reimbursement purposes.

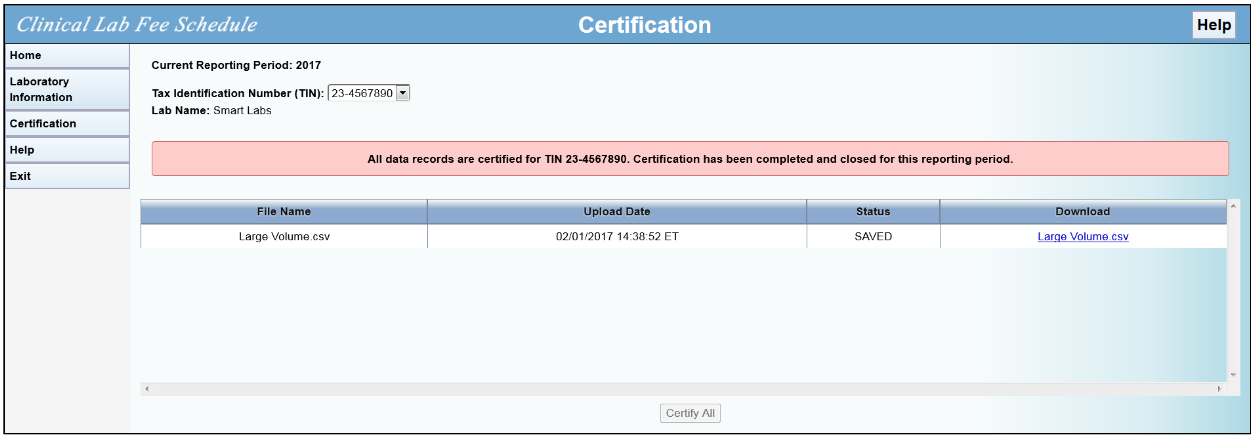
☐ **I agree to the above certification statement**

4. Review the statement, click in the box next to "I agree to the above certification statement," and then click on the **Certify** button.

   Note: The application will display a message "All data records are certified. Certification has been completed and closed for this reporting period."

   The "Results" for the data file changes "SAVED" to "CERTIFIED" as shown in Figure 7-11.

Figure 7-11: Certification - Data Certified Window – Large Volume/Very Large Volume



Current Reporting Period: 2017

Tax Identification Number (TIN): 23-4567890

Lab Name: Smart Labs

All data records are certified for TIN 23-4567890. Certification has been completed and closed for this reporting period.

File Name	Upload Date	Status	Download
Large Volume.csv	02/01/2017 14:38:52 ET	SAVED	Large Volume.csv

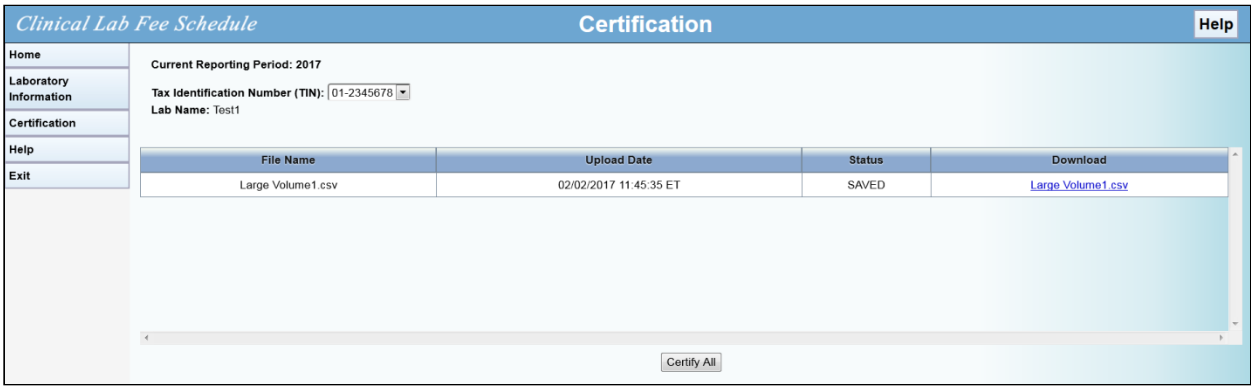
Warning: Once the CLFS Certifier has certified the data for the current period, data submission is closed, and no more data can be entered for that applicable laboratory. Be sure that all applicable information is entered, accurate, and complete before certifying the data. If corrections need to be made post certification, please contact the CLFS helpdesk:

Application Help Desk

- E-mail: CLFSHelpDesk@dcca.com
- Phone: 844-876-0765
  - 9AM-6PM Eastern, Non-Peak
  - 9AM-9PM Eastern, Peak (i.e., January-March 2017)

5. To certify data for another TIN, select another TIN from the TIN dropdown menu, as shown in Figure 7-12.

Figure 7-12: Certification – Certify Another TIN – Large Volume/Very Large Volume



Current Reporting Period: 2017

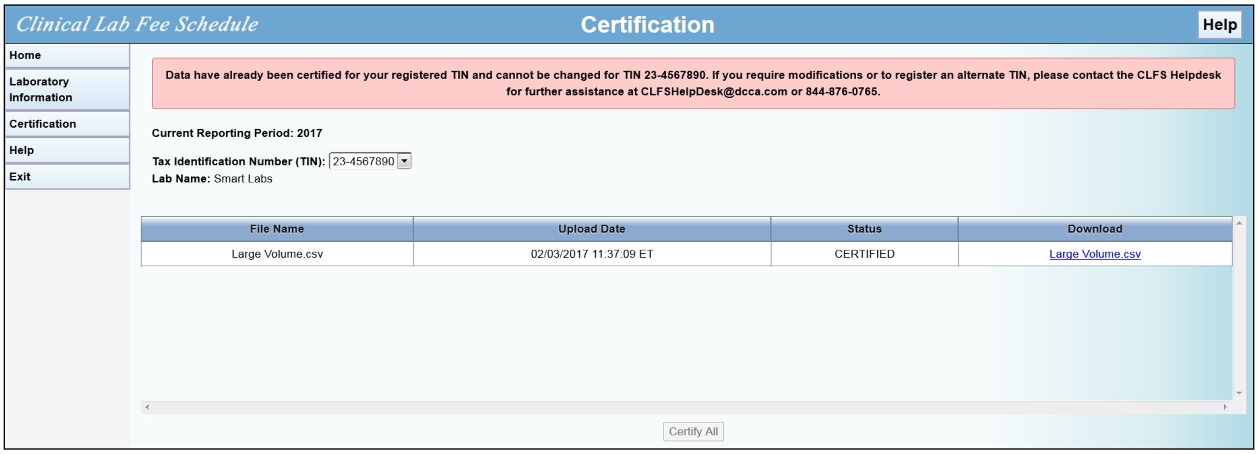
Tax Identification Number (TIN): 01-2345678

Lab Name: Test1

File Name	Upload Date	Status	Download
Large Volume1.csv	02/02/2017 11:45:35 ET	SAVED	Large Volume1.csv

Note: if you select a TIN where data have already been certified, you will receive a message stating that the data have already been certified for the selected TIN, as shown in Figure 7-13.

Figure 7-13: Certification – Selected TIN has Already Been Certified Message



Data have already been certified for your registered TIN and cannot be changed for TIN 23-4567890. If you require modifications or to register an alternate TIN, please contact the CLFS Helpdesk for further assistance at CLFSHelpDesk@dcca.com or 844-876-0765.

Current Reporting Period: 2017

Tax Identification Number (TIN): 23-4567890

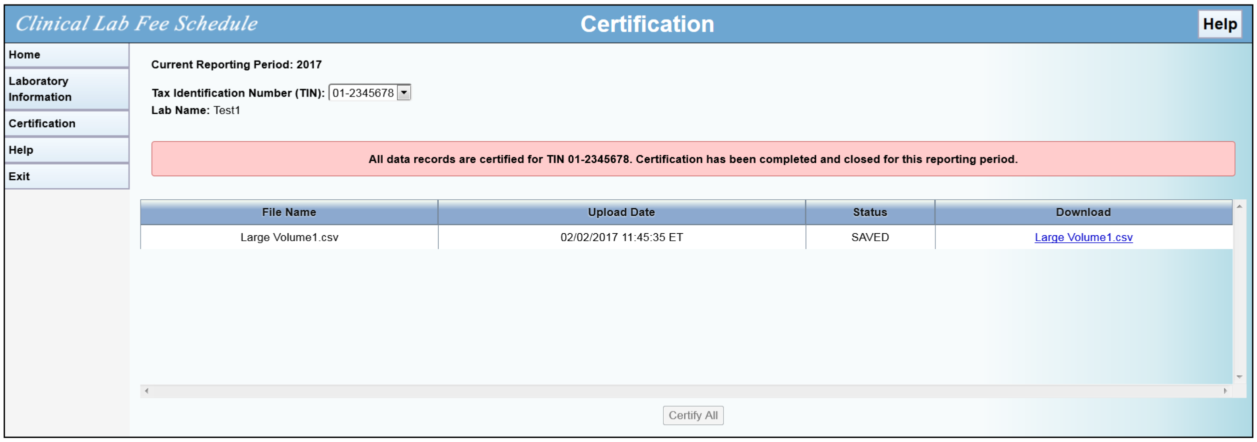
Lab Name: Smart Labs

File Name	Upload Date	Status	Download
Large Volume.csv	02/03/2017 11:37:09 ET	CERTIFIED	Large Volume.csv

6. Click on the **Certify All** button and repeat step 4.

   All the “Results” for the data changes are changed from being “SAVED” to “CERTIFIED,” as shown in Figure 7-14.

Figure 7-14: Certification - Data Certified Window – Large Volume/Very Large Volume



Current Reporting Period: 2017

Tax Identification Number (TIN): 01-2345678

Lab Name: Test1

All data records are certified for TIN 01-2345678. Certification has been completed and closed for this reporting period.

File Name	Upload Date	Status	Download
Large Volume1.csv	02/02/2017 11:45:35 ET	SAVED	Large Volume1.csv

8. Frequently Asked Questions

8.1 General

1. **What is the CMS Enterprise Portal?**

   The CMS Enterprise Portal is a convenient single point of entry to numerous CMS applications, systems, and databases.

2. **Who is eligible to have a CMS User Account?**

   All US citizens who are over 18 years of age and have a valid US residential address are eligible to have a **CMS User Account**.

3. **Who do I contact for Portal Login issues?**

   CMS Portal login issues should be directed to “our helpdesk info.”

8.2 Supported Browsers

1. **What browsers are supported by the CMS Enterprise Portal?**

   The CMS Enterprise Portal supports the following browsers:

   - Internet Explorer (IE) 11
   - Firefox
   - Chrome
   - Safari

2. **What browser mode is supported?**

   There are different browser modes that can be specified by you, the user. Only the native browser mode is supported. To find out what browser mode you are using, hit the F12 key while in IE. The top of the resulting window/panel will show the browser mode being used.

3. **What document mode is supported?**

   There are different document modes that can be specified by you, the user. Only the native document mode is supported. To find out what document mode being used, hit the F12 key while in IE. The top of the resulting window/panel will show the document mode being used.

4. **Is JavaScript required for the CMS Enterprise Portal?**

   JavaScript needs to be enabled for successful use of the Enterprise Portal.

8.3 Personal Information

1. **What personal information is required to provide to register for my user account?**

   You must provide your legal name, current home address, primary phone number, and e-mail address. You must enter your first and last name as they appear in legal documents, such as your driver's license or passport. If you have a suffix included in your name (such as Sr., Jr., II, etc.), make sure you select it from the suffix field exactly as it appears on legal documents.

2. **Why should I submit personal information to create a user account and how safe is it?**

   IDM collects personal information to uniquely identify users when registering with the system. We may also use your answers to the challenge questions and other PII to later identify you in case you forget or misplace your User ID/Password. For security level information please visit: Centers for Medicare & Medicaid Services (CMS) Website Privacy Policy.

3. **Can I register for an IDM user account with a foreign address and an international phone number?**

   Yes, IDM allows users to register with a foreign address and an international phone number. At a minimum, foreign addresses must include the following information:

   - House number, street name, and country; and
   - An international phone number that must start with the country code, followed by the area code, and the primary phone number.

4. **Can I change my foreign address to a U.S. address, and vice versa?**

   Yes, IDM allows users to change their address from a foreign address to a U.S. address, and vice versa. Use the 'Change Address' link under the 'My Profile' menu to change your address.

5. **What will you do with my PII?**

   IDM uses an external authentication service provider, Experian, to verify your identity based on the information you provide. Experian verifies your information against its records to successfully identify you. CMS provides, on public-facing websites, their Terms & Conditions of how your information will be handled when registering for a CMS IDM user account.

6. **How many days do I have to confirm my IDM account?**

   IDM requires users to confirm their account between 30 and 180 days. Accounts are confirmed by selecting the link provided to the user in their account confirmation e-mail. If the user fails to confirm their account, then the link and the account will expire.

7. **How can I update my personal information?**

   You can update your personal information by selecting 'My Profile' from the dropdown menu at the top right-hand corner of the CMS Portal home page. You will then be directed to the 'View My Profile' page, where you can change your personal information by selecting the links on the right side of the page. You may be requested to answer challenge questions based on the changes you make.

8. **Where can I find information regarding who has the right to request a Social Security Number (SSN)?**

Federal law mandates that State departments of motor vehicles, tax authorities, welfare offices, and other governmental agencies request your SSN as proof that you are who you claim to be. However, the Privacy Act of 1974 requires that any government agency requesting your SSN provide details on how this information will be used, and what law or authority requires its use.

For information on who has the right to request your SSN please select the following link: Who Can Lawfully Request My Social Security Number?

The Privacy Act can be read at the following link: The Privacy Act of 1974.

9. **I already provided my personal information during registration to setup an IDM user account. Why do I have to provide it again to access certain applications?**

   When you have selected an application or role that requires a higher level of security, you are required to complete Identity Verification. In most cases, you may need to provide a few more details (i.e., SSN, Date of Birth) to be able to request access to the selected application or role.

10. **Will my SSN be shared with any federal or private agency?**

    Your SSN will be used for verification purposes only. IDM does not share your SSN with any other federal or private agency.

11. **How often do I need to update my password?**

    IDM requires that users update their password at least once between 60 days and 24 months depending on the user role community. Once your password expires, you will be prompted to enter your new password. You can use the ‘Change Password’ self-service feature located on the ‘My Profile’ page. To use this feature, you must sign into the CMS Portal and select the ‘My Profile’ link from the dropdown menu at the top right-hand corner of the CMS Portal home page. You must click the ‘Change Password’ link on the ‘My Profile’ page to change your Password.

8.4 Identity Verification

1. **What is Identity Verification?**

   Identity Verification is the process of providing sufficient information (e.g., identity history, credentials, or documents) to a service provider for the purpose of proving that an individual is who he/she claims to be. Individuals requesting electronic access to CMS protected information or systems must be identity proofed prior to being given access.

2. **Why does Experian require my personal information?**

   Experian uses your personal information to verify your identity against your personal information record.

3. **Does verifying my identity by Experian affect my credit score?**

   No, this kind of inquiries is known as a “soft inquiry.” Soft inquiries do not affect your credit score, and there are no charges related to them. Soft inquiries are displayed in the consumer version of the credit profile, which is neither viewable nor reported to lenders. If you order a credit report from Experian, you will see an entry of inquiry by the CMS Medicaid Services with CMS’ address on the date the request was made.

4. **Will I be required to go through Identity Verification after changing my address from foreign address to U.S. home address and vice versa?**

No, you will not be required to re-do Identity Verification if you already have a role that previously required your identity to be verified.

5. **What if I have problems completing Identity Verification? Is there an Experian Help Desk?**

   Yes, Experian Verification Support Services is a dedicated call center for individuals who have failed the online Remote Identity Proofing (RIDP) process while attempting to obtain a CMS IDM user account. If you fail online RIDP, IDM will generate a reference code and the Experian Verification Support Services contact information will be provided on the screen for further action.

6. **What happens if the Experian Help Desk cannot verify my identity?**

   If your identity cannot be verified, even with assistance from the Experian Help Desk, you will need to contact your application specific Help Desk to go through a document-based proofing process. If your Application Help Desk cannot verify your identity, your access to CMS applications that require a higher level of security will be restricted.

7. **Why am I not able to change my User ID?**

   The User ID identifies you uniquely to IDM; therefore, you cannot change your User ID.

8. **Can I use the same credentials for different applications?**

   Yes, you may use the same credentials to access different applications. Once you have logged into the CMS Portal home page, you can request access to other applications.

9. **When I try to login, I get an error message “Incorrect combination of User ID or Password. Please try again. If you need further assistance, you may use the “Forgot User ID” or the “Forgot Password” link to help you.” What should I do?**

   Please check the user ID and password that you entered. An incorrect combination of these will result in such an error message.

10. **When I try to login, I get an error message “Incorrect combination of User ID, Password or Security Code. Please try again. If you need further assistance, you may use the “Forgot User ID” or “Forgot Password” links to help you. For issues with the Security Code, you may use the "Unable to Access Security Code?" link or contact your Application Help Desk.” What should I do?**

    Please check the user ID, password, and Security Code that you entered. An incorrect combination of these will result in such an error message.

11. **When I try to log in, I am prompted to enter a Security Code. What do I do if I don’t have an MFA device registered to my account or am having issues retrieving a Security Code?**

    For issues with logging in with a Security Code you may use the following options:

    - If you do not have an MFA device registered to your account, you may use the “Register MFA Device” link on the Password and Security Code page for assistance.
    - If you are unable to retrieve a Security Code from your registered MFA device or do not have your device available, you may use the “Unable to Access Security Code?” link on the Password and Security Code page for assistance.
    - If you have trouble using the “Register MFA Device” or “Unable to Access Security Code?” links, you may contact your Application Help Desk for assistance.

For more information about MFA, please refer to section 9.5 Multifactor Authentication (MFA)

12. **When I try to log in, I get the error message stating "Your account is disabled. Contact the Help Desk to enable your account." Why does this happen?**

    A user's account can be disabled by Application Help Desks or by IDM Administrators for possible reasons that are linked to security violations or fraud detection. To enable your disabled account, you are required to contact the Application Help Desk.

13. **When I try to log in, I get the error message stating "Your account has been locked. Please try again later." Why did this happen and how can I get my account unlocked?**

    After three unsuccessful attempts to login, your account will be locked. Your account will be unlocked after 60 minutes have elapsed since your third consecutive failed authentication attempt. After the 60 minutes have passed, you will be required to enter valid credentials associated to your user account to unlock the account. If you are unable to unlock your account, you may call your Application Help Desk for assistance.

14. **When I try to log in, I am directed to the 'Unlock My Account' view. Why is this and how do I unlock my account?**

    IDM locks your user account if no account activity is reported for 60 days. When you login after 60 days the system will display the 'Unlock my Account' view; enter your User ID and correctly answer all challenge questions on the next page; enter your old password and then a new password in the input fields of 'New Password' and 'Confirm New Password' to unlock your account.

15. **What are challenge questions and why do I need to select and answer them when setting up my account?**

    IDM uses challenge questions for security purposes to verify your account. When you register your account, you will need to select three different questions and provide an answer for each question. You will be asked to answer the challenge questions in the future if you forget your password, change your address, change your phone number, or to unlock your account. Correct responses to the challenge questions will enable IDM to confirm your account.

8.5 Multifactor Authentication (MFA)

1. **What is MFA?**

   MFA is a type of login (authentication) that, in addition to a user ID and password, requires another "factor" such as a Security Code. To comply with CMS policy, most users will need to establish a second login "factor" commensurate with the level of access requested. CMS uses Symantec's Validation and Identity Protection (VIP) service to add a second layer of protection for your online identity. Symantec provides VIP through computer, phone, and e-mail.

2. **How do we use MFA?**

   You will be asked to enter your user ID, password, and an additional Security Code that is generated by Symantec VIP software to gain access to your application. The Security Code can be generated by:

   - A free Symantec application that can be downloaded to your desktop or Smartphone.

- An SMS or Interactive Voice Response (IVR) once you have registered your phone in your application; or
- By e-mail.

The “Where can I get the MFA software?” section below provides the necessary information to install the Symantec application on your desktop or Smartphone.

3. **How do I get an MFA device?**

   Your application will prompt you to register an MFA device when you request access to protected information, and you have not already registered an MFA device with the application. You will be given a choice of MFA Security Code delivery methods. The primary MFA Security Code delivery method is to download software and install it on your computer or a mobile device. Alternatively, if you require special support, you can set up SMS or IVR to deliver your MFA Security Code. Details on where to get the MFA software are described below.

4. **Where can I get the MFA software?**

   You will need MFA software if you choose to receive your MFA Security Code on a computer, laptop, or mobile device. You will be required to download the MFA software from Symantec and install it on your device of choice.

   To download the desktop software for Windows or Mac, go to the Validation and IP Protection Center and follow the instructions.

   If using an iPhone, Android, Blackberry, or other mobile device, use your device to navigate to Validation and ID Protection Mobile Center and follow the instructions.

   SMS, IVR, and e-mail options do not require a software download.

5. **When I click on an application, I am redirected to the MFA login screen. What is this?**

   The MFA login screen is displayed when you attempt to access an MFA-protected application. If you have an MFA device, you will be able to access the application. If you do not have an MFA device, then you will have to register for MFA using either your phone or computer.

6. **What are the types of devices I can register with for my MFA?**

   You can add one or more of the following devices as your MFA device:

   - Smartphone, Computer, or Tablet – By downloading the Symantec VIP access application.
   - IVR – By registering with a U.S. phone number.
   - SMS – By registering with a U.S. phone number; and
   - E-mail – By registering with a valid e-mail address (the e-mail address associated with your profile will be used).

7. **How do I register my MFA device (phone, computer, or e-mail) to my IDM user account?**

   Once you successfully complete the Identity Verification process, IDM will display the ‘Register your Phone, Computer, or e-mail’ page depending on the application role being requested. Alternatively, you can register for MFA by selecting the ‘Register your Phone, Computer, or e-mail’ link under ‘My Profile’.

   Your device can be registered for MFA in one of five ways:

   a. Download VIP access software on your phone – Enter the alphanumeric Credential ID generated by the VIP access client. Then enter the Security Code generated by the VIP client.

   b. Download VIP access software on your computer – Enter the alphanumeric Credential ID generated by the VIP access client. Then enter the Security Code generated by the VIP client.

   c. Text Message SMS – Use this option to have the Security Code texted to your phone. You must enter a valid phone number and your phone must be capable of receiving text messages. Carrier charges may apply.

   d. IVR – Use this option to receive a Voice Message containing the Security Code. You must provide a valid phone number and (optional) extension that will be used during login to obtain the Security Code. The extension may begin with any one of the following: asterisks ‘*’; period ‘.’; comma ‘,’; pound ‘#’, followed by numeric 0 to 9. For example: 4885554444, 1112.

      - * (asterisk) Used by some phone systems to access extension.
      - . (period) Creates a delay of approximately 5 seconds.
      - , (comma) Creates a short delay of approximately 2 seconds.
      - # (pound) Used by some phone systems to access an extension; and
      - A comma may be used if you are unsure of the special character supported by your company’s phone system.

   e. e-mail – You can also opt to use the e-mail in your profile to receive a Security Code when logging into a secure application.

8. **How do I register for MFA if I receive an error when installing the software on my computer?**

   If you are having trouble downloading and installing the MFA software on your desktop or laptop, it is possibly due to your company’s Information Technology (IT) policy that disables users from installing any software on company-provided machines. Check with your company’s IT department for assistance. If your company does not allow you to install MFA software, one alternative is to use a mobile device that you control, or you can also use a voice call to obtain the Security Code. You can refer to other instructions in this FAQ section for information on cell phone installation and IVR usage.

9. **I cannot use the desktop MFA software or the mobile phone MFA software. What should I do?**

   Your application allows you to set up a voice or SMS delivery method for your Security Code that does not require an MFA software download. You can register a phone number and select SMS or IVR. Then your application can register your phone number and delivery method with Symantec. After your MFA is activated, when you login to your application you will receive either a phone call or text message that contains your Security Code, depending on the delivery method you selected.

   The SMS and IVR Security Codes expire within 10 minutes of when they are sent, so please make sure you provide a phone number that will be accessible to you during your typical work hours. For example, do not use a residential phone number if you will normally login from your place of employment. E-mail Security Codes expire within 30 minutes of when they are sent.

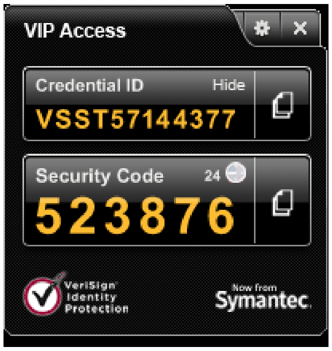
10. **Can I access multiple applications if I'm Multi-Factor Authenticated (MFA)?**

    Once you have been multi-factor authenticated (i.e., "logged in") into your application, if you do not log out of the system, you can access other protected CMS Applications that require MFA without having to be authenticated again with an MFA Security Code. If you log out of the system, when you log back in, you will be asked to present your MFA Security Code when accessing your CMS Application.

11. **How do I use my MFA device to log into my CMS IDM user account?**

    When you log into your application, the system will display the MFA login screen. You will be required to enter your user ID, password, and the MFA Security Code. If you have registered an MFA device, enter your user ID, password, and the Security Code that is displayed on your MFA device, as shown in Figure 9-1.

Figure 9-1: Security Code



VIP Access

Credential ID VSST57144377

Security Code 523876

For your protection, an MFA device automatically generates a new Security Code each time it counts down from a 30-second timer.

If you have registered an MFA SMS or IVR device, when you log into your application, the system will send you a Security Code via text message or voice call to the number you registered in IDM.

For your protection a Security Code sent via SMS or IVR counts down from a 10-minute timer. The Security Code sent via e-mail counts down from a 30-minute timer.

12. **How do I add additional MFA devices to my CMS IDM user account?**

    You can register up to five MFA devices to your user account. Additional MFA devices can be added to your account after you have been prompted by your application to set up the first MFA device. The “Register your Phone, Computer, or e-mail” link on the “My Profile” page will appear once you have successfully set up your first MFA device. You can click on the link and add additional MFA devices to your user account.

13. **Will I be charged cell phone time each time I use Symantec VIP MFA on my mobile device?**

    It depends on what delivery method you use. The Symantec VIP MFA software is free. Once the Symantec VIP MFA application is downloaded and installed on the phone it does not utilize any cell time to generate the six-digit security code. Cell or network traffic is used to download the application to one’s mobile device. There are no recurring charges associated with the use of either software option. If you choose not to use the software option and select SMS or IVR, carrier charges may apply.

14. **I lost all my MFA devices linked to my IDM user account. How do I deactivate the linked devices and link new devices to my user account?**

    Your Application Help Desk should be able to assist you in removing/deactivating the registered devices and registering new devices to your user account.

15. **What should I do if I lock my MFA device?**

    You must contact your Application Help Desk to unlock the registered MFA device.

16. **If my Credential ID is copied or stolen, can someone else access my CMS IDM User account?**

    No. A Credential ID cannot be used to access an IDM user account.

8.6 Annual Certification

1. **What does it mean when my account is inactive?**

   A CMS Portal account is inactive when a user has not logged into either their application or the CMS Portal for 60 days or more.

2. **What does it mean when my account is locked?**

   A user’s account is locked following 60 days of inactivity. The user is prevented from logging into any application. To unlock an account the user must: login to the CMS Portal, answer their challenge questions, and reset their password; or call the Application Help Desk.

3. **What does it mean when my account is deleted?**

   When a user’s CMS Portal account does not have a role in any application and has been inactive for more than 360 days it will be deleted. The user’s account may no longer be used for any purpose and the user may register again to create a new account.

4. **What is an Account Review?**

   Users wishing to acquire a role in their application must first register for a CMS Portal account. Account Reviews are conducted every six months to check for the presence of at least one application role in a user’s account. If an account does not have any application roles associated to it and has been inactive for more than 180 days, it will fail. If the account has been inactive for more than 360 days, it will be deleted.

5. **Is there anything I need to do for Account Reviews?**

   If you have an application role associated to your account, then no action is required on your part. If you do not have an application role associated to your account and have been inactive for more than 180 days, you will receive an e-mail with instructions on how to proceed.

6. **I got an e-mail that my account failed an Account Review. What should I do next?**

   If you no longer require an account in the CMS Portal, no further action is required on your part. If you wish to continue using your account, please follow the instructions in the e-mail describing how to proceed.

7. **I got an e-mail that my account was deleted as part of an Account Review. What should I do to get my account back?**

   If your account was deleted as part of Account Review, you must create a new account. Please go to the CMS Portal and follow the on-screen instructions to create a new account.

8. **What is a Role?**

   A Role is the name (e.g., Submitter or Representative) given to a set of privileges and permissions that an individual may perform within an application or other computer resource. Users must submit a role request which should be approved and then the role will be added to the user's profile. Use of a role is typically granted for one year by an application Business Owner, their representatives, authorizers, Help Desk personnel, or other approver. Each year continued use of a role must be approved or the role will be removed from the user's profile. This annual re-approval is known as Annual Certification.

9. **What is Annual Certification?**

   CMS security guidelines require that each year, the use of a role must be approved, or the role will be removed from the user's profile. Annual Certification is the process of approving a user's continued use of a role and is valid for one year. Annual Certification is typically performed in the same manner as the original role approval process used by Business Owners, their representatives, authorizers, Help Desks, or other approvers. If the continued use of a role is not approved, then the role will be removed from the user's profile and an e-mail will be sent notifying the user that their role has been removed.

10. **What is an Annual Certification due date?**

    The Annual Certification due date is the date that a role is due to be certified. This is normally one year after the last Annual Certification.

11. **How often does my role need to be certified?**

    Your role needs to be certified once a year. It is your approver's responsibility to certify your role and usually requires no action on your part.

12. **What do I need to do to have my role certified?**

    It is your approver's responsibility to certify your role and usually requires no action on your part. If your role failed Annual Certification, an e-mail will be sent to you with more information.

13. **I got an e-mail that my role was removed because it failed Annual Certification. How do I get my role back?**

    If you still need access to the role that was removed, you must request the role again. Please follow the instructions provided in the e-mail.

14. **I am an approver who is responsible for approving role requests. What do I need to do for Annual Certification?**

    As an approver for role requests, you will be responsible for certifying users' roles by the certification due date. An 'Annual Certification' link can be found where you usually go to approve user role requests. On that page you will be able to search, review, certify, or revoke the certifications for users under your authority. If no action is taken by the certification due date, the role will be removed.

15. **I am an approver, and I received an e-mail informing me that I have roles pending Annual Certification. What do I need to do?**

    As an approver for users' role requests, you are also responsible for certifying those roles annually. 30 days before a role's certification due date, you will receive an e-mail providing a count of user roles that are due for certification within the next 30 days, 15 days, 7 days, and 1 day. If no action is taken by the certification due date, the role will be removed.

16. **If my role is automatically approved, do I need to take any action for Annual Certification?**

    If your role requests are automatically approved, they will also be automatically certified. Some automatically approved roles require the information provided, when the role was first requested, to be validated against a trusted resource. As part of Annual Certification, this information will need to be revalidated. If the validation is successful, your role will be certified automatically, and no action is required on your part. If the validation fails, CMS.gov will send you an e-mail notifying you that validation failed and describing how to correct the error before the certification due date for your role.

17. **Why can't I see all my users' roles in the Pending Certification View Page?**

    The Pending Certification View Page shows a maximum of 250 roles that you are responsible for certifying in the next 30 days. If you have more than 250 roles to certify in the next 30 days or wish to see roles due for certification past the next 30 days, you must use the Search feature.

18. **I am searching for roles that I need to certify but don't see any results after selecting the Search button. Why is my search not displaying any results?**

    The most likely reason is that your search did not match any existing role certifications. The search will also not return any results if there are more than 250 certifications found for your specific search criteria. Please ensure that you narrow down your search so that no more than 250 certifications will be found from your search request.

Appendix A: Acronyms

Table 1: Acronyms

Acronym	Literal Translation
ADLT	Advanced Diagnostic Laboratory Test
ARS	Acceptable Risk Safeguards
CCN	CMS Certification Number
CDLT	Clinical Diagnostic Laboratory Test
CFO	Chief Financial Officer
CLFS	Clinical Laboratory Fee Schedule
CM	Center for Medicare Management
CMS	Centers for Medicare & Medicaid Services
IDM	Identity Management
EIN	Employer Identification Number
EUA	Enterprise User Administration
FAQ	Frequently Asked Questions
FFSDCS	Fee for Service Data Collection System
HCPCS	Healthcare Common Procedure Coding System
IE	Internet Explorer
IT	Information Technology
IVR	Interactive Voice Response
LV	Large Volume
NPI	National Provider Identifier
OTP	One Time Password
PAMA	Protecting Access to Medicare Act
PFS	Physician Fee Schedule
PII	Personal Identifiable Information
PTAN	Provider Transaction Access Number

Acronym	Literal Translation
RIPD	Remote Identity Proofing
SMS	Short Message Service
SSN	Social Security Number
TIN	Tax Identification Number
URL	Uniform Resource Locator
VIP	Validation and Identity Protection
VLV	Very Large Volume